

pureMDM - Benutzerhandbuch

Version 1.14.3.0

RDS Consulting GmbH
Mörsenbroicher Weg 200
40470 Düsseldorf

Kontakt
Telefon +49 (211) 968 56.0
Telefax +49 (211) 968 56.34
info@rds.de
www.rds.de

Bankverbindung
Bankhaus Lampe KG
BLZ 480 201 51
Konto 1 531 999

Commerzbank AG
BLZ 300 800 00
Konto 602 518 300

UniCredit Bank AG
BLZ 360 201 86
Konto 14 768 807

Umsatzsteuer-ID-Nr.
DE 120585553

Geschäftsführende
Gesellschafterin:
Sandra Gehling

Registergericht Düsseldorf
HRB 30228



Kontaktdaten

Bei Rückfragen oder Anregungen nutzen Sie bitte die unten stehende E-Mail-Adresse oder Telefonnummer.

E-Mail:

mobilesupport@rds.de

Telefon:

+49 (211) 96 85 6 - 18



INHALTSVERZEICHNIS

1 ANMELDUNG AN PUREMDM

Für die Nutzung von pureMDM ist ein Internet-Browser notwendig. Unterstützt werden Microsoft IE (ab Version 7.x), Mozilla Firefox und Apple Safari. Nach dem Start des Browsers ist die URL über die Adresszeile einzugeben.

Die Eingabe des Kennwortes ist Case-sensitiv. Nach Eingabe des Benutzernamens und Kennworts ist die Schaltfläche „Anmelden" zu aktivieren.

Die Anmeldung an pureMDM wird, sowohl bei Erfolg als auch bei Misserfolg, von dem System protokolliert. Bei nicht erfolgreicher Anmeldung wird der Grund für die Abweisung im Protokoll hinterlegt.

Bitte beachten Sie, dass Sie nach zwanzig Minuten Inaktivität automatisch ausgeloggt werden.

Die Startseite von pureMDM zeigt, gemäß der Berechtigungsrolle des Anwenders, unterschiedliche Funktionen.

Es stehen die Funktionen „Mitarbeiter verwalten", „Geräte verwalten" „Gerät ausrollen (Schnellerfassung)" und „Gerät ausrollen" zur Verfügung. Über Erstere gelangen Sie zu der Mitarbeiterliste, über die Sie die bereits registrierten Mitarbeiter verwalten sowie neue hinzufügen können. Die zweite Funktion öffnet die Geräteliste und bietet die Möglichkeit bereits eingebundene Geräte zu verwalten und neue auszurollen. Die beiden letzten Funktionen erlauben das Ausrollen einzelner Geräte. Die Sichten dieser Funktionen werden im folgenden Abschnitt näher beschrieben.

Das Dashboard zeigt eine Übersicht aller mit pureMDM verwalteten Geräte. Anhand dessen kann der Administrator, in Form eines Diagramms, den Status der Geräte auf einen Blick sehen. Sobald das System manipulierte Geräte feststellt, sieht der Administrator ein weiteres Diagramm, welches alle manipulierten Geräte zeigt.

2 MENÜSTRUKTUR VON PUREMDM

In diesem Kapitel erhalten Sie einen Überblick über die einzelnen Bereiche und Funktionen von pureMDM.

Die Navigationsleiste auf der linken Seite ist in die Bereiche Datenpflege und Auswertungen unterteilt. Der entsprechende Bereich kann per Mouseover eingeblendet und fixiert werden.

2.1 Datenpflege – Aufgaben

Die Menüpunkte „Gerät ausrollen (Schnellerfassung)" sowie „Gerät ausrollen" erlauben das Ausrollen einzelner Geräte, sowie das Erfassen der Geräte- und Mitarbeiterdaten. Der Umfang der erfassten Daten ist der Aspekt, in welchem sich die beiden Funktionen voneinander unterscheiden. Bei der Schnellerfassung eines Geräts müssen beispielsweise die IMEI-Nummer und die Seriennummer nicht eingegeben werden. Diese Daten können dann bei Bedarf zu einem späteren Zeitpunkt ergänzt werden.

Die Felder „Vertrag" und „Mitarbeiter" lassen sich zur Eingabe eines neuen Datensatzes erweitern. Diese Möglichkeit besteht nur wenn entsprechende Berechtigungen vorhanden sind.

1. Betriebssystem:
   Auswahl des Betriebssystems des Mobile Devices per Dropdown-Menü.
2. Vertrag:
   Eingabe der mobilen Rufnummer. Der Eintrag ist zur Differenzierung nach Vorwahl, Hauptnummer und Anbieter erweiterbar.
3. Mitarbeiter:
   Eingabe des Benutzers des mobilen Gerätes.
   Der Eintrag ist erweiterbar zur Differenzierung nach Vor- und Nachname, Benutzername, E-Mail und Standardsprache.
4. Registrierungscode:
   Auswahl der Übermittlung des Registrierungscodes.
5. Gruppe:
   Auswahl zu welcher Gruppe (siehe 3.5) das mobile Gerät hinzugefügt werden soll.

6. Name:
   Eingabe eines Gerätenamens.

2.2 Datenpflege – Organisation

Im Bereich „Organisation" erfolgt die Verwaltung der Mitarbeiterdaten. Er ist in die Funktionen „Meine Daten", „Mitarbeiter", „Abteilungen", „Meine Firma", „Berechtigungsrollen" und „Kostenstellen" unterteilt. Diese werden im Folgenden beschrieben.

2.2.1 Meine Daten

Der Bereich „Meine Daten" gibt dem aktuell angemeldeten Benutzer Einsicht in seine persönlichen Daten und erlaubt es ihm diese zu ändern, insofern diese nicht automatisch durch eine Active Directory Integration synchronisiert werden. Es ist dem Benutzer beispielsweise möglich das eigene Kennwort für pureMDM zu ändern oder das eigene Gerät zu verwalten. Die Funktionen, die dem Benutzer angezeigt werden, sind abhängig von seiner Berechtigungsrolle.

Die Benutzer können ihre persönlichen Daten in den Eingabefeldern ändern. Die Änderungen werden durch das Aktivieren der „Speichern"-Schaltfläche wirksam. Beachten Sie bitte, dass die Daten bei einer vorhandenen Active Directory Synchronisation mit dem Active Directory ihres Unternehmens abgeglichen werden. Eine manuelle Änderung wird in diesem Falle durch die Synchronisation überschrieben. Sie können die Schaltfläche „Kennwort ändern" zum Ändern Ihres pureMDM-Kennworts verwenden. Es wird eine Maske eingeblendet, in der Sie die Möglichkeit haben ein neues Kennwort festzulegen.

Eigene Geräte können in dieser Sicht über die Schaltfläche „Gerät hinzufügen" in das System aufgenommen werden. Die Sicht wechselt nach aktivieren der Schaltfläche in die „Gerät ausrollen"-Maske (Abschnitt 2.1).

Eigene, bereits ausgerollte Geräte werden in dem unteren Bereich „Meine Geräte" aufgelistet. Je nach zugewiesener Berechtigungsrolle (siehe hierzu Abschnitt 2.2.5) ist eine Verwaltung möglich. Man kann, zwecks Rollout, für seine Geräte einen Registrierungscode generieren und entfernen. Dies geschieht über den Drop-Down-Menüpunkt „Gerätebenachrichtigung". Generierte Codes werden im Eintrag des Gerätes angezeigt. Ein Code kann direkt im Afaria Client eingegeben werden, sofern das Gerät noch nicht

ausgerollt wurde. Nachdem das System den Code verifiziert hat, beginnt die Rolloutprozedur, die das Gerät in das zentrale Management aufnimmt.

Der Drop-Down-Menüpunkt „Sicherheit" erlaubt das Sperren und Entsperren des Gerätes, wobei das Sperren auf dem Gerät die Anforderung des Gerätecodes zum Entsperren auslöst. Entsperren wird genutzt, um einen Gerätecode, welcher vom Anwender vergessen wurde, zurückzusetzen, so dass ein neuer Code vergeben werden kann. Das Entfernen des Gerätes aus der Kontrolle von pureMDM bedeutet, dass die zentral durch pureMDM konfigurierten Daten, z.B. PIM Daten vom Gerät gelöscht werden. Das Gerät befindet sich nach diesem Schritt nicht mehr unter der Kontrolle des Systems. Der Eintrag in der Geräteliste (siehe Abschnitt **Fehler! Verweisquelle konnte icht gefunden werden.**) muss, falls benötigt, dort manuell gelöscht werden. Beachten Sie bitte, dass ein Löschen des Geräteeintrages dementsprechend in der Sicht „Meine Geräte" nicht möglich ist. Dies ist nur in der Geräteliste möglich. Ein „Gerät auf Werkseinstellungen zurückzusetzen" bedeutet das Löschen aller in dem Gerät gespeicherten Daten. Ein Gerät befindet sich nach Ausführen des Befehls wieder im Aktivierungsmodus.

Bei Android Geräten, auf welchen die NitroDesk TouchDown App installiert ist, kann der Speicher per Fernbefehl gelöscht werden. Auch der von TouchDown angelegte Speicherbereich auf der Speicherkarte kann gelöscht werden.

2.2.2 Mitarbeiter

Die Mitarbeiterliste zeigt alle in pureMDM angelegten Benutzer, unabhängig davon, ob ein Gerät zugeordnet ist. Bei manueller Anlage oder Datenimport können die Einträge einzelner oder mehrerer Benutzer verändert, hinzugefügt und gelöscht werden.

Falls eine Active Directory Synchronisation eingesetzt wird, besteht die Gefahr, dass diese die Änderungen in den Benutzerdaten überschreibt. Aus diesem Grund sollten die Daten direkt im Active Directory gepflegt werden.

Alle im System vorhandenen Mitarbeitereinträge werden in der Liste dargestellt. Mittels der Seitenzahlen kann in der Liste geblättert werden. Eine Sortierung der angezeigten Einträge ist durch das Anklicken der Spaltenüberschriften möglich. Über die Suchfunktion (Lupen-Symbol) kann auch eine Filtrierung bzw. Selektion der Einträge vorgenommen werden.

Bitte beachten Sie, bei der Eingabe der Daten, dass alle fettgedruckten Felder Pflichtfelder sind.

Neben den persönlichen Daten des Mitarbeiters können auch sein Eintritts- und Austrittsdatum sowie die Zeitzone in der er sich befindet, definiert werden. Der letztgenannte Eintrag ermöglicht es pureMDM die Zeitstempel in den Datensichten automatisch an die relevanten Zeitzonen anzupassen.

Über den Reiter „Berechtigungen" besteht die Möglichkeit dem neuen Benutzer eine oder mehrere Benutzerrollen zuzuweisen. Dies geschieht über das Auswählen der Berechtigungsgruppe in dem Bereich „Alle Gruppen" und das Verschieben in den Bereich „Mitglied von" mittels der Pfeil-Schaltfläche. Die Mitgliedschaft in der Rolle „public" kann nicht entfernt werden, diese grundlegende Rolle wird allen Benutzern zugewiesen. Der Mitarbeitereintrag wird durch Aktivieren der „Speichern"-Schaltfläche gespeichert. Beim erstmaligen Speichern eines neuen Mitarbeitereintrags wird auch ein Zeitstempel für die Erstellung hinterlegt.

Die dem Benutzer zugeordneten Zertifikate und Geräte werden auf zusätzlichen Reitern aufgelistet.

Bestehende Einträge können über das neben stehende Editiersymbol (Person mit Bleistift) geöffnet und bearbeitet werden.

Die Funktion „Export" exportiert die Liste in das Excel-Dateiformat oder als CSV-Datei. Ein Massenimport auf Basis einer CSV-Datei ist über den Button „Import" durchführbar. Dieser Vorgang wird in den Abschnitten 3.1.1.1, 3.1.2.1 und 3.1.2.3 detailliert behandelt. Zudem können Mitarbeiterdaten optional auch mit Ihrem Active Directory synchronisiert werden.

2.2.3 Abteilungen

Hier erfolgt die Pflege der Abteilungen. Es besteht die Möglichkeit das Unternehmen anhand seines Organigramms abzubilden. Bei der Anlage kann neben dem Namen, einem Leiter, einer Kostenstelle und Beschreibung der Abteilung auch eine Standard Gerätegruppe ausgewählt werden. Diese Gerätegruppe enthält die Konfigurationen, welche für alle Geräte dieser Abteilung gelten sollen. Sie vererben die Standardgruppe der von der obersten Abteilung auf die darunterliegenden Gerätegruppen, indem Sie die Funktion „Standardgruppe für alle untergeordneten Abteilungen" aktivieren.

Durch das Aktivieren der Schalflächen „Neu parallel" und „Neu untergeordnet" werden parallele bzw. untergeordnete Abteilungen erstellt. Bitte beachten Sie, dass der Leiter, die Kostenstelle und die Gerätegruppe schon angelegt sein müssen, bevor sie einer Abteilung zugewiesen werden können. Eine detailliertere Beschreibung der Anlage von Abteilungen finden Sie in Abschnitt 3.1.2.2. Die Hierarchie von Abteilungen kann per Verschieben und Ablegen geändert werden.

Bestehende Abteilungen können durch die Auswahl des jeweiligen Eintrags geöffnet und editiert werden.

2.2.4 Meine Firma

Auf dieser Seite werden die Firmeninformationen wie Name, Adresse, Land und Standardsprache hinterlegt und verändert. Die Netzwerkinformationen der Netbios und LDAP-Domäne sollten zwingend richtig sein, wenn Sie pureMDM mit Ihrem Active Directory synchronisieren.

Sie haben weiterhin die Möglichkeit Ihr eigenes Firmenlogo in die Titelleiste von pureMDM einzubinden. Zusammen mit der Option, deren Farbe zu definieren (siehe Abschnitt 2.7.1), ist somit eine Anpassung von pureMDM an Ihre Corporate Identity möglich.

2.2.5 Berechtigungsrollen

In diesem Bereich werden die Berechtigungsrollen verwaltet. Es können Rollen hinzugefügt, bearbeitet und gelöscht werden. Diese weisen Sie den einzelnen Benutzern über den Mitarbeiter-Bereich zu. Das Definieren und Zuweisen von Berechtigungsrollen erlaubt eine sehr genaue Kontrolle, auf welche Bereiche von pureMDM Ihre Mitarbeiter zugreifen dürfen.

Folgende Rechte können für normale Benutzer festgelegt werden:

- Lese-Rechte („Lesen")
- Einfüge-Rechte („Einfügen")
- Ändern-Rechte, („Ändern")
- Lösch-Rechte („Löschen")
- Einsicht in die Historien und Protokolle („Historie")
- Die Webservice-Zugriffsrechte dienen dem Zugriff auf das System durch die Webservice-Schnittstelle.

Die Bereiche und Zugriffsrechte sind in einem Raster dargestellt. Durch das Aktivieren der jeweiligen Optionen können Sie für jeden Bereich von

pureMDM Zugriffsrechte definieren. Beachten Sie bitte, dass Sie bei der Auswahl höherer Rechte niedrigere automatisch aktivieren z.B. wird das „Lesen"-Recht bei dem Aktivieren des „Ändern"-Rechtes automatisch mitaktiviert. Eine bestehende Rolle kann durch einen Klick auf das Editier-Symbol (Schlüsselsymbol mit Bleistift) neben dem Eintrag geöffnet und auf gleichem Wege editiert werden.

2.2.6 Kostenstellen

Sie können Kostenstellen hinzufügen, löschen, exportieren und importieren. Die Zuweisung von Kostenstellen ermöglicht eine spätere Auswertung pro Kostenstelle.

Sie können einen Kostenstellenverantwortlichen, Beschreibungen der Kostenstellen sowie den Zeitraum in denen sie aktiv sind hinterlegen.

Vorhandene Kostenstellen können Sie per Klick auf das Editiersymbol (Euro-Symbol mit Bleistift) öffnen.

2.3 Datenpflege – Geräte

Der Bereich „Geräte" organisiert und verwaltet die mobilen Geräte und Ihre Anwender, deren Gruppen und die dazugehörigen Gerätekonfigurationen.

2.3.1 Mobile Geräte - Geräteliste

Die Geräteliste zeigt Informationen zu den Geräten sowie deren Status an. Sie können mobile Geräte hinzufügen, löschen, exportieren und importieren. Sortieren Sie die Spalten durch Anklicken der Spaltenüberschriften. Ein Klick auf das Lupen-Symbol öffnet die Suchmaske. Die linke Seite zeigt den Gerätestatus. Das „Schild"-Symbol signalisiert, wenn ein Gerät vom System zugelassen wurde. Die Ampel zeigt den Zeitbereich an, wie lange sich ein Gerät nicht mit dem System verbunden hat. Die genaue Zeit wird per Mouseover angezeigt. Das Intervall, nach welchem der Verbindungsstatus wechselt, kann sowohl gruppenspezifisch in der Gerätegruppe als auch systemweit in den System-Einstellungen definiert werden. Der Status eines Geräts kann in drei verschiedene Kategorien eingeordnet werden, Rot, Gelb und Grün.

Die obere Symbolleiste enthält Schaltflächen zur Bearbeitung der Listeneinträge. Die durch das Lupen-Symbol geöffnete Suchmaske dient der Suche nach Geräten und erlaubt eine Filterung der Einträge nach bestimmten

Kriterien. Das Drop-Down-Menü „Aktionen", oberhalb der Geräteliste, erlaubt das Generieren und Senden von Registrierungscodes per Push-Nachricht in Form von E-Mails und SMS.

Die beiden letzten Schaltflächen bieten eine Ex- und Import-Funktionalität. (zu Letzterem siehe auch Abschnitt 3.1.1.4).

Unterhalb der Geräteliste gibt es ebenfalls einige Drop-Down-Menüpunkte. Hier kann der Administrator:

Aktionen durchführen

- das Erlauben eines Sim-Kartenaustausches kann festgelegt werden
- ein gerätespezifisches Dokument anhand einer Vorlage erstellen

Gerätebenachrichtigungen versenden

- „Sende Einstellungen" erlaubt eine sofortige manuelle Übertragung der Gerätekonfiguration an ein Gerät. Ansonsten würde dies zu den, in den Systemeinstellungen festgelegten, Intervallen stattfinden (siehe Abschnitt 2.7.1).
- das Generieren eines Registrierungscodes. So können Sie Geräte auch per Code-Eingabe in dem Afaria Client ausrollen. Der Code wird dann in der Geräteliste sowie im Geräteeintrag, angezeigt. Er ist nur für das angezeigte Gerät sowie den ausgewählten Mandanten gültig, kann für das zugewiesene Gerät aber mehrfach verwendet werden.
- Generieren und Senden des Registrierungscodes per Mail oder SMS an den Benutzer.

Bitte beachten Sie, dass alle drei letztgenannten Menüpunkte nach dem Generieren bzw. dem Generieren und Versenden deaktiviert sind. Ein neuer Registrierungscode kann erst wieder generiert werden, wenn der alte Code mit dem Menübefehl „Gerätebenachrichtigung/Entferne Registrierungscode" gelöscht wurde.

Sicherheit

- das Sperren und Entsperren eines Geräts
- das Entfernen aus der Kontrolle
- das Zurücksetzten auf Werkseinstellungen
- NitroDesk Daten löschen
- NitroDesk und SD-Karten Daten löschen

Das Ausführen dieser Aktionen wird unter dem Reiter „Protokoll" registriert.

Im unteren Bereich können Sie Einträge einzelner Geräte bearbeiten. Ein Klick auf das Editieren-Symbol (Gerät mit Bleistift) öffnet die Ansicht der Daten des ausgewählten Gerätes. Im ersten Reiter werden die allgemeinen Gerätedaten angezeigt. Der Reiter „Geräteinformationen" zeigt die Informationen an, welche der Afaria Client auf dem jeweiligen System gesammelt hat. Hierzu gehören die folgenden Informationen über das Gerät und seine Konfiguration. Beachten Sie, dass einige dieser Daten geräteplattform-spezifisch sind.

- Afaria
  Liefert Informationen über den installierten Afaria Client und dem Betriebssystem des Geräts
- Bluetooth
  Beschreibt Eigenschaften über die Bluetooth-Schnittstelle des Geräts
- Certificates
  Listet die auf dem Gerät installierten Zertifikate auf
- Device
  Liefert technische Informationen über das Gerät
- Memory
  Information über die Speicherauslastung
- MS Exchange
  Auf dem Gerät installierte Exchange-Konten
- Payloads
  Führt die auf dem Gerät durch das MDM installierten Konfigurationen auf
- Phone
- Information über das Telefon-Modul
- Restrictions
  Listet die dem Betriebssystem von dem MDM auferlegten Restriktionen auf
- Security
  Liefert Daten über die Gerätesicherheit
- Wi-Fi
  Daten über die Wi-Fi Schnittstelle des Geräts

Der Reiter „Software" zeigt die auf dem System installierte Software, während der Reiter „Protokoll" eine Liste der an dem Gerät durchgeführten Aktionen und Maßnahmen anzeigt.

2.3.2 Gerätegruppen

Sie können in den Gerätegruppen eine oder mehrere Gerätekonfigurationen zu einer Gerätegruppe zusammenfassen. Gerätekonfigurationen können nur mit Hilfe von Gerätegruppen an mobile Geräte versendet werden. Aus dieser Sicht können die Geräte der ausgewählten Gruppe auch direkt benachrichtigt werden, per SMS oder Push-Nachricht, um Änderungen sofort wirksam zu machen. Dies geschieht mittels des Menüs „Gerätebenachrichtigung".

Definieren von Ampelzeiten

Für jede Gruppe können optional Zeiten für die Statusampel definiert werden. Falls dies nicht erfolgt würde die systemweite Einstellung (vorzunehmen in den Systemeinstellungen) greifen.

Gerätekonfiguration

Auf der linken Seite sind alle bereits erstellten Gerätekonfigurationen zu sehen. Die rechte Seite zeigt alle ausgewählten und somit zur Gerätegruppe hinzugefügten Gerätekonfigurationen. Das Hinzufügen und Entfernen wird mit Hilfe der Pfeile in der Mitte umgesetzt. Sich aufhebende bzw. widersprüchliche Gerätekonfigurationen in einer Gruppe werden vom System nicht akzeptiert.

Software

Auf gleiche Weise können auch Einträge aus der Softwareliste (siehe auch Abschnitt 2.5.1) zugewiesen werden. Auch das Zuweisen gesamter Software-Kategorien ist möglich.

Enrollment

Unter diesem Reiter können iOS Geräte der Gruppe, welche manipuliert wurden, zum MDM zugelassen werden. Für iOS und Android Geräte kann die Option, ein Identity/x.509 Zertifikat zu nutzen, aktiviert werden. Für Windows Phone Geräte kann das Verbindungsintervall festgelegt werden. Dieser Wert kann jedoch nur einmal, während des Rollouts, für das jeweilige Gerät definiert werden. In dem Bereich „Enrollment Variablen" können Variablen festgelegte werden, deren Werte während des Rollouts vom Anwender festgelegt werden können und anschließend in Konfigurationen genutzt werden können.

2.3.3 Gerätekonfigurationen

In der Gerätekonfiguration können Sie alle für die Geräte verfügbaren Regeln, Restriktionen, Konfigurationen, Workflows und Business-Logiken erstellen und verwalten. Das Erstellen und Zuweisen von Gerätekonfigurationen wird in Abschnitt 3.5 beschrieben.

Zur Auswahl stehen die im Folgenden beschriebenen Konfigurationen für die mobilen Betriebssysteme Android, iOS und Windows Mobile Professional/ Standard. Im Fall von iOS werden die Gerätekonfigurationen als Richtlinien übertragen, welche nach dem Empfang automatisch auf dem Gerät installiert werden. Gerätekonfigurationen können in dem Hauptmandanten definiert und über die Funktion „In allen Firmen bereitstellen" an Untermandanten verteilt werden.

In Textfeldern können z.T. Variablen verwendet werden. Die Auswahl der verfügbaren Variablen wird angezeigt, wenn ein Prozentzeichen als erstes Zeichen im Eingabefeld eingegeben wird.

In iOS-Konfigurationen für Active Sync, VPN und Wifi können Zertifikate z.B. für die Authentifizierung angegeben werden. Hier werden drei verschiedene Möglichkeiten angeboten:

1. Direkte Angabe eines Zertifikates
2. Konfiguration einer SCEP-Anfrage
3. Auswahl einer Zertifikatsvorlage

Die dritte Möglichkeit wird nur angeboten wenn Zertifikate mit dem ADSync-Dienst hochgeladen wurden. Es werden alle verwendeten Zertifikatsvorlagen als Auswahl aufgeführt. Für die Konfiguration von Zertifikaten aus Zertifikatsvorlagen lesen Sie bitte die Dokumentation des ADSync Dienstes.

2.3.3.1 Konfiguration (Android)

Diese Konfiguration erlaubt das komplette Einstellen von Android Smartphones und Tablets.

Geräteinventur

Erlaubt es dem Afaria Client, Information über das Gerät sowie der auf dem Gerät installierten Software zu sammeln und an pureMDM zu übertragen. Diese Information wird in den jeweiligen Geräteeinträgen und den Auswertungen angezeigt. Zudem können die Automatismen von pureMDM auf diese Ereignisse reagieren.

Sicherheit

Erlaubt das Erzwingen von Passwörtern sowie das Definieren von deren Eigenschaften. Darüber hinaus können Sie festgelegen, nach wie vielen fehlgeschlagenen Anmeldeversuchen das Gerät auf Werkseinstellung zurückgesetzt wird.

Heartbeat

Das Zeitintervall definiert, nach welchem das Gerät seine Inventurdaten bei pureMDM abliefert und überprüft, ob neue Richtlinien für das Gerät vorhanden sind. Falls ein Verbindungsversuch fehlschlägt, kann festgelegt werden wie oft das Gerät versuchen soll die Verbindung erneut aufzubauen.

Bluetooth

Die Drahtlos-Übertragungs-Schnittstelle Bluetooth wird aktiviert bzw. deaktiviert. Dies ist auch unter dem „Samsung"-Reiter möglich; die Einstellung sollte, je nach den verwendeten Geräten, nur unter dem jeweiligen Reiter erfolgen.

WLAN

Erlaubt es Ihnen, die WiFi-Verbindung zu aktivieren und zu konfigurieren. Die WiFi-Aktivierung ist unter dem „Samsung"-Reiter möglich und sollte nur an einer Stelle erfolgen. Das Hinterlegen des Sicherheits-Schlüssels erspart Ihren Anwendern das spätere Eintippen desselben.

NitroDesk

Die Sandbox-App NitroDesk TouchDown wird über den Reiter „NitroDesk" konfiguriert. Anpassen können Sie den App-eigenen Passwortschutz, Synchronisations-Einstellungen sowie diverse PIM- und Sicherheits-einstellungen.

Motorola

Unter dem Reiter „Motorola" lassen sich diverse Einstellungen für Motorola Geräte konfigurieren. Hervorzuheben ist hier die Möglichkeit ein Exchange Konto festzulegen sowie ein VPN zu konfigurieren.

Samsung

Der Reiter „Samsung" kann zur Konfiguration von Samsung Galaxy Geräten genutzt werden. Hier gilt es zu beachten, dass die Aktivierung von Passwortschutz, Bluetooth sowie WiFi auch in anderen Reitern erfolgen kann.

Bei einem gemischten Gerätebestand sollten diese Einstellungen unter den anderen Reitern erfolgen, um Konflikte zu vermeiden. Ggf. kann es sinnvoll sein mehrere Richtlinien für mehrere Geräte, je nach Hersteller zu erstellen.

2.3.3.2 Gerät Root-Prüfung (Android)

Diese Gerätekonfiguration legt den Automatismus fest, welcher angestoßen wird, falls das System auf einem Android Gerät ein „Rooting" feststellt. Mögliche Aktionen sind das Versenden von E-Mails an den Benutzer und/oder den Administrator sowie das Löschen der Daten aus dem Gerät. Ein Entfernen aus der Kontrolle von pureMDM ist, wie im Gegensatz bei dem äquivalenten Automatismus für iOS Jailbreaks, nicht möglich.

2.3.3.3 Passcodeüberwachung (Android)

Mit dieser Konfiguration kann ein Workflow definiert werden, welcher ausgelöst wird, wenn die Kennwortrichtlinien auf dem Gerät nicht den Richtlinien der zugewiesenen Konfiguration entsprechen. Auch hier sind die Aktionen E-Mail-Benachrichtigung, Sperren des Gerätes, Löschen der Daten aus dem Gerät sowie das Entfernen des Gerätes aus der Kontrolle des Systems verfügbar.

2.3.3.4 Konfiguration (iOS)

APN-Einstellungen (iOS)

Diese iOS Gerätekonfiguration erlaubt das Festlegen des Zugangspunktes (Access Point Name, APN) sowie der Zugangsdaten und des Proxy Servers.

CalDAV (iOS)

Mit der CalDAV-Gerätekonfiguration kann ein CalDAV-Server definiert werden, um Kalender-Daten zu synchronisieren.

CardDAV (iOS)

Diese Gerätekonfiguration ähnelt der CalDAV-Gerätekonfiguration, nur dass hier ein CardDAV-Server definiert wird.

Zertifikate (iOS)

Diese Konfiguration überträgt ein beliebiges Zertifikat an die Geräte.

E-Mail (iOS)

Einrichtung eines POP3 und/oder eines IMAP E-Mailkontos.

Passcode (iOS)

Der Passwortschutz des iOS Gerätes wird mit dieser Konfiguration vorgegeben. Die Art und Länge des Passworts sowie dessen Gültigkeitsdauer, können Sie hier ebenfalls festgelegen. Die Einstellung „Maximale Anzahl fehlgeschlagener Versuche" bestimmt, nach wie vielen fehlgeschlagenen Versuchen sich das Gerät auf Werkseinstellungen zurückgesetzt.

Provisioning Dateien

Gerätefunktionalität (iOS)

Mittels dieser Gerätekonfigurationen können Sie bestimmte Aktionen und Funktionen auf iOS Geräten verhindern bzw. deaktivieren. Dies betrifft in erster Linie die von dem iOS Betriebssystem bereitgestellten Funktionen und Anwendungen sowie das Verbinden mit Apples iCloud Dienst.

SCEP (iOS)

Richten Sie in dieser Gerätekonfiguration eine Verbindung zu einem SCEP-Server ein.

Einstellungen

Subscribed Calendar (iOS)

In dieser Konfiguration kann über eine URL ein Kalender abonniert werden.

VPN (iOS)

Konfigurieren Sie eine VPN-Verbindung mittels L2TP, PPTP oder IPSec. Um das Hochladen von Benutzerzertifikaten zu konfigurieren lesen Sie bitte die Hilfe welche mit dem ADSync-Tool mitgeliefert wird.

Webclips (iOS)

Auf dem iOS-Homescreen können Sie Verknüpfungen zu Webseiten, samt Icon hinterlegen (Web Clips). Sie können Icons hochgeladen und den Text, welcher unter dem Icon angezeigt wird festgelegen.

WiFi (iOS)

Konfiguration eines WiFi-Netzwerks. Falls mehrere Netzwerk-Zugänge auf den Geräten benötigt werden, müssen Sie pro Verbindung eine Konfiguration anlegen. Um das Hochladen von Benutzerzertifikaten zu konfigurieren lesen Sie bitte die Hilfe welche mit dem ADSync-Tool mitgeliefert wird.

2.3.3.5 Jailbreak-Erkennung (iOS)

Für den Fall das auf einem iOS Gerät ein Jailbreak ausgeführt wird, kann mittels dieser Konfiguration ein Automatismus definiert werden, der bei Erkennung des Jailbreaks durchgeführt wird. Zur Erkennung von Jailbreaks muss auf den Geräten ein Custom Afaria Client installiert sein. Zu den möglichen Aktionen gehören E-Mail-Benachrichtigungen an den Administrator und/oder den Benutzer, das Sperren des Gerätes, das Löschen der Daten aus dem Gerät sowie das Entfernen des Gerätes aus der Kontrolle des Systems. Letzteres beinhaltet auch das Entfernen aller Einstellungen und Firmendaten aus dem Gerät. Bitte beachten Sie, dass die E-Mail-Benachrichtigung das Einrichten der jeweiligen E-Mail-Vorlagen benötigt (siehe Abschnitt 2.7.2).

2.3.3.6 Konfiguration (Windows Mobile Professional)

Für Windows Mobile Geräte gibt es, Android ähnlich, eine einzige Gerätekonfiguration, welche das gesamte Gerät konfiguriert. Diese ist auch in Reiter unterteilt.

Geräteinventur

Erlaubt das Übertragen von Inventurdaten des Gerätes an pureMDM

Verbindung

Hier lassen sich eine RAS-Verbindung, Wählstandorte sowie die IP- und DNS-Einstellungen konfigurieren.

Formate

Wie das Windows Mobile Betriebssystem Länderspezifische Zahlen, Währungen und Zeiten darstellen soll, kann man unter dem Reiter „Formate“ definieren.

Netzwerk

Hier können Benutzerdaten sowie die Domäne hinterlegt werden. Stellen Sie in dem Bereich „Windows Mobile Update“ die Verfahrensweise für das automatische Update ein.

Besitzer

Legt den Besitzer des Geräts sowie Informationen zum Unternehmen fest.

Ton

Definieren Sie die maximale Lautstärke unter dem Reiter „Ton". Dort weisen Sie auch dem Betriebssystem eigene Töne für Ereignisse oder Eingaben-Feedback zu.

Benutzer-Zugriffsrechte

Diese Einstellungen betreffen in erster Linie das Ausführen von Programmen auf dem Gerät.

Roaming Kontrolle

Erlaubt die Regulierung des Daten-Roamings sowie die Benachrichtigung des Anwenders bei Beginn und Ende des Roamings.

Provisionierung

Gibt Ihnen die Möglichkeit einzustellen, ob und welche Software auf Geräte verteilt wird.

2.3.3.7 Konfiguration (Windows Phone)

Die Konfigurationsmöglichkeiten von Windows Phone 8 Geräten beschränken sich momentan auf die folgenden Punkte:

Inventory

Hier kann festgelegt werden, ob Hardwaredaten ausgelesen werden. Ein Auslesen der installierten Software ist nicht möglich.

Active Sync

Unter diesem Punkt kann ein Exchange Konto auf dem Gerät installiert werden.

Passcode

Diese Einstellungen ermöglichen das Festlegen von Richtlinien für den Gerätepasscode.

2.3.3.8 Software-Überwachung (Allgemein)

Diese Gerätekonfiguration ermöglicht, in Verbindung mit den Einträgen in der Software Liste (siehe Abschnitt 2.5.1), das Whitelisting der Anwendungen auf den Geräten. Falls eine Anwendung auf einem Gerät erkannt wird, die nicht in der Liste enthalten ist bzw. nicht dem Gerät zugeordnet ist, dann greifen die in der Konfiguration definierten Workflows. Zu diesen gehören das Benachrichtigen von Benutzer und/oder dem Administrator per E-Mail, das

Sperren des Gerätes, das Löschen der Daten aus dem Gerät sowie das Entfernen des Gerätes aus der Kontrolle des Systems.

2.3.3.9 Software Sperrlisten-Überwachung (Allgemein)

Bei dem Einsatz dieser Gerätekonfiguration werden die auf einem Gerät entdeckten Anwendungen mit denen auf der Software Sperrliste eingetragenen (siehe Abschnitt 2.5.3) verglichen (Blacklisting). Falls es eine Übereinstimmung gibt, wird der in der Konfiguration definierte Workflow ausgeführt. Auch hier sind die Aktionen E-Mail-Benachrichtigung, Sperren des Gerätes, Löschen der Daten aus dem Gerät sowie das Entfernen des Gerätes aus der Kontrolle des Systems verfügbar.

2.3.3.10 Software Installationsüberwachung

Diese Konfiguration prüft, ob die von dem Administrator empfohlenen Anwendungen auch auf dem Gerät installiert wurden. Die Anwendungen müssen in der Software-Liste entsprechend als erforderlich gekennzeichnet werden. Bitte beachten Sie, dass in der empfohlenen Software immer der App-Identifier eingetragen ist, weil sie sonst nicht erkannt werden kann. Der Workflow wird ausgeführt falls eine der erforderlichen Apps auf dem Gerät fehlt. Dieser kann sich aus den Aktionen E-Mail-Benachrichtigung, Sperren des Gerätes, Löschen der Daten aus dem Gerät sowie das Entfernen des Gerätes aus der Kontrolle des Systems zusammensetzen.

2.3.3.11 SIM-Kartenüberwachung (Allgemein)

Mit dieser Konfiguration kann ein Workflow definiert werden, der durch einen SIM-Kartenwechsel ausgelöst wird. Auch hier sind die Aktionen E-Mail-Benachrichtigung, Sperren des Gerätes, Löschen der Daten aus dem Gerät sowie das Entfernen des Gerätes aus der Kontrolle des Systems verfügbar.

2.3.3.12 Prüfung Mitarbeiter verlässt Unternehmen (Allgemein)

Diese Gerätekonfiguration implementiert einen Workflow, welcher ausgeführt wird, wenn ein Anwender ein ausgerolltes Gerät besitzt und er gesperrt wird oder sein Vertrag ausläuft (dieser Statuswechsel kann auch von dem AD ausgelöst werden). Auch hier sind die Aktionen E-Mail-Benachrichtigung, Sperren des Gerätes, Löschen der Daten aus dem Gerät sowie das Entfernen des Gerätes aus der Kontrolle des Systems verfügbar. Die Konfiguration kann mit einer entsprechenden Vorlage dazu genutzt werden, den Mitarbeiter auf das Zurückgeben seines Gerätes hinzuweisen.

2.3.3.13 Überwachung Betriebssystemversion (iOS und Android)

Mit dieser Konfiguration kann ein Workflow definiert werden, der durch eine nicht zertifizierte Betriebssystem-Version auf einem Gerät ausgelöst wird. Die Liste der zertifizierten Version wird durch Semikolon getrennt angegeben. Ein Sternchen als letztes Zeichen kann als Platzhalter angegeben werden. Auch hier sind die Aktionen E-Mail-Benachrichtigung, Sperren des Gerätes, Löschen der Daten aus dem Gerät sowie das Entfernen des Gerätes aus der Kontrolle des Systems verfügbar.

2.3.4 Globale Zertifikate

Unter diesem Bereich können global-gültige Zertifikate eingepflegt werden, welche über eine Zertifikats-Policy an die Geräte verteilt werden können. Anwendungsbeispiele wären hier der Einsatz von einem Root-Zertifikat oder der Einsatz von Zertifikaten für die gruppen-basierte Geräte-Authentifizierung.

2.4 Datenpflege – Verträge

Dieser Bereich erlaubt die Verwaltung der Mobilfunkverträge, welche Geräten (nicht zwingend) zugewiesen werden müssen. Ein Vertrag ist wiederum mit einem Tarif verbunden, welcher seinerseits einem Mobilfunkanbieter zugeordnet ist. Diese Beziehungen können Sie festgelegen. Zu beachten ist: Es muss mindestens ein Tarif angelegt werden, damit auch ein Vertrag angelegt werden kann.

2.4.1 Vertragsliste

In der Vertragsliste werden alle in pureMDM eingetragenen Verträge mit den Feldern „Vorwahl“, Rufnummer („Nummer“), „Tarif“ und Laufzeit („Beginn“ und „Ende“) angezeigt. Zusätzlich können Sie „Bemerkungen“ (Freitext) eintragen. Es können Verträge hinzugefügt, bearbeitet, gelöscht, exportiert und importiert werden. Dabei muss beachtet werden, dass der ausgewählte Tarif bereits angelegt sein muss. Die Anlage von Verträgen per Datenimport wird in dem Abschnitt 3.1.2.5 beschrieben. Neben den allgemeinen Vertragsdaten können unter dem Reiter „Details“ auch Informationen für einen Service Desk, wie Super-PINs, hinterlegt werden

2.4.2 Tarife

Der Menüpunkt „Tarife“ bietet die Möglichkeit alle im Unternehmen verfügbaren Tarife mit den entsprechenden Laufzeiten und Bezeichnungen zu

hinterlegen. Tarife können hinzugefügt, bearbeitet, gelöscht und exportiert werden. Jeder Tarif wird einem Mobilfunkanbieter zugeordnet, dessen Eintrag muss hierfür in der Datenbank angelegt sein.

2.4.3 Mobilfunkanbieter

Im diesem Bereich können Sie die hinterlegten Mobilfunkanbieter einsehen. Diese können von Ihnen nur bearbeitet werden, wenn pureMDM lokal im Kundennetzwerk installiert ist. Sie können die Liste jedoch exportieren. Bitte kontaktieren Sie RDS Mobile Support falls Sie Änderungen oder Neuerungen wünschen.

2.5 Datenpflege – Software

Der Bereich „Software" gibt Ihnen die Möglichkeit, Ihren Mitarbeitern Applikationen, welche im Google Play Portal oder im Apple App Store erhältlich sind, vorzuschlagen. Darüber hinaus können Sie eigen entwickelte Enterprise-Apps zwecks deren Installation auf die Geräte verteilen. Auf die Verteilung der Enterprise-Apps folgt eine Benachrichtigung in dem Afaria Client, auf die der Benutzer mit dem Start der Installation agieren muss. Über eine Sperrliste lassen sich Ihre Geräte auf nicht gestattete Anwendungen hin überwachen.

2.5.1 Software

In diesem Bereich wird die über pureMDM zur Verfügung gestellte Software verwaltet. Bei der Betrachtung von iOS Anwendungen wird zwischen den beiden Kategorien „iPhone App Store Anwendung" und „iPhone Enterprise Anwendung" unterschieden. Bei App Store Anwendungen wird dem mobilen Gerät durch den Afaria Client eine Verknüpfung zum Apple App Store zur Verfügung gestellt. Die Software kann dann über die entsprechende Apple App Store Seite heruntergeladen werden. Eine Enterprise Anwendung ist eine vom Unternehmen entwickelte und bereitgestellte Software. Diese wird ohne den Apple App Store direkt zur Installation zur Verfügung gestellt. Aufgrund einer Änderung in den Apple Richtlinien wird, seit Ende 2011, die Installation von Enterprise Apps bei dem Start des Afaria Clients vorgeschlagen; die Apps werden nicht mehr in diesem aufgelistet.

Die gleiche Unterscheidung existiert auch für Android Geräte; auch dort gibt es Enterprise und Google Play Anwendungen. Das Anlegen von Einträgen in der Softwareliste wird in Abschnitt 3.6.1 beschrieben. Einträge in der

Softwareliste können in dem Hauptmandanten definiert und über die Funktion „In allen Firmen bereitstellen“ in allen Untermandanten bereitgestellt werden. In diesen können die Einträge sofort den jeweiligen Gruppen zugeordnet werden.

2.5.2 Software-Kategorien

Sie können eigene Kategorien zur Differenzierung der bereitgestellten Software erstellen. Diese werden auf das mobile Gerät übertragen und ermöglichen im Afaria Client eine Filterung der verfügbaren Software.

2.5.3 Software Sperrliste

Die Software Sperrliste erlaubt das sogenannte Blacklisting. Falls Anwender bestimmte Anwendungen nicht auf den mobilen Geräten installieren sollen, können Sie besagte Anwendungen in der Sperrliste eintragen. Das Pflegen einer Whitelist, die zugelassene Apps aufführt, erfordert weniger Aufwand als die Pflege einer Blacklist. Blacklisting empfehlen wir für Bring Your Own Device Programme. Für unternehmenseigenen Geräte eignet sich eher das Whitelisting. Falls eine der eingetragenen Anwendungen auf einem Gerät erkannt wird, so greift der in der Gerätekonfiguration „Software Sperrlisten-Überwachung“ definierte Workflow (siehe Abschnitt 2.3.3.9).

2.6 Datenpflege Protokolle

In dem Bereich „Protokolle“ sind zwei Listen aufrufbar, welche beide die Anmeldungen am System protokollieren.

Anmeldeprotokoll Benutzer

In der ersten Liste werden die Anmeldungen durch normale Benutzer dokumentiert. Schlägt die Anmeldung eines bekannten Benutzers fehl, wird auch dies dokumentiert, gemeinsam mit dem Grund der Ablehnung durch das System.

Anmeldeprotokoll Webservice

Das zweite Protokollenthält die Anmeldungen durch Dienste, wie den Active Directory Synchronisierungsdienst.

In beiden Protokollen werden Informationen über den Zeitpunkt, Benutzername, Erfolg, Ursache, Browser, Hostname und die Adresse angezeigt.

2.7 Datenpflege – Einstellungen

Das Menü „Einstellungen" bietet Ihnen den Zugriff auf alle wichtigen Einstellungen, mit denen Sie Ihre pureMDM-Umgebung, den Bedürfnissen Ihres Unternehmens entsprechend, konfigurieren können.

2.7.1 Systemeinstellungen

In den Systemeinstellungen können Sie die systemnahen Einstellungen Ihren Bedürfnissen anpassen.

Verknüpfungen auf Startseite

Auf der Startseite können Sie dem Benutzer Verknüpfungen z.B. auf weiterführende Informationen hinterlegen. Fügen Sie neue Zeilen durch Drücken des „+-„-Symbols hinzu, entfernen Sie Zeilen mit dem Kreuz. URLs müssen mit dem Protokoll" http" oder „https" vollständig angegeben werden, ist dieses nicht angegeben wird automatisch „http" vorangestellt.

Globale Variablen für Textvorlagen

Globale Variablen können für E-Mail oder Dokumentenvorlagen definiert werden. Fügen Sie neue Zeilen durch Drücken des „+-„-Symbols hinzu, entfernen Sie Zeilen mit dem roten Kreuz.

Support

Diese Felder erlauben das Hinterlegen von Support-Kontaktinformationen auf dem User-Self-Service-Portal.

Hintergrundverarbeitung

Die Intervalle für die Hintergrundverarbeitung legen fest, nach wie vielen Stunden die Übertragung der Konfigurationen an die Geräte und die Geräteüberwachung jeweils wiederholt werden. Ersteres erlaubt das automatisierte Aktualisieren von Konfigurationen auf allen Geräten. Dies kann pro Betriebssystem ein oder abgeschaltet werden. Beachten Sie, dass Sie die Konfiguration einzelner Geräte auch über deren Eintrag in der Geräteliste manuell aktualisieren können (Menüoption „Gerätebenachrichtigung/Sende Einstellungen"). Mit Letzterer werden die Workflows angestoßen, falls der für den Workflow definierte Gerätestatus erreicht wurde. Beachten Sie, dass dies auch die Häufigkeit der von dem System versendeten Statusmails festlegt.

Mobile Geräte

Unter der Rubrik „Mobile Geräte" kann eine Standard-Gerätegruppe definiert werden. Hier können Sie die Art und Weise festlegen in der pureMDM den Verbindungsstatus der einzelnen Geräte anzeigt. Die Zeitspanne, nachdem der jeweilige Status wechselt, kann hierfür definiert und eingetragen werden.

Oberfläche

In der nächsten Rubrik, „Oberfläche" können Sie Anpassungen am Aussehen der pureMDM-Benutzeroberfläche vornehmen. Anpassbar sind die Beschriftungen und die Hintergrundfarben der Titelleiste. Dies erlaubt das Verwenden eines Titels, welcher zu Ihrer Corporate Identity passt. Die Farbe wird mit RGB-Werten definiert.

Attributeinstellungen

Die Rubrik, „Attributeinstellungen" ermöglicht das Festlegen des Geräte-Felds „IMEI" und des Vertrags-Felds „SIM-Kartennummer" als Pflichtfelder. Zudem kann die IMEI-Nummer der Geräte optional überwacht werden. Im Rahmen dieser IMEI-Überwachung wird bei einem Rollout die IMEI des Gerätes mit der in pureMDM hinterlegten IMEI verglichen. Das System verhindert den Rollout, falls die IMEI- oder Seriennummern nicht übereinstimmen und protokolliert den Vorfall im Geräteeintrag unter dem Reiter „Protokoll" in der Protokollliste.

2.7.2 Einbinden von Geräten

Die allgemeinen Einstellungen erlauben es, mandantenweit die Gültigkeitsdauer der Registrierungscodes festzulegen. Nach Ablauf der Gültigkeitsdauer eines Registrierungscodes kann ein Gerät nicht mehr mit diesem ausgerollt werden. Auch die Nachrichtenvorlage, welche für das Versenden von Registrierungscodes per Push- und SMS-Nachrichten verwendet werden soll, kann hier festgelegt werden (siehe auch Abschnitt 2.7.6).

Unter dem Punkt „Abfragen während des Ausrollens" können mandantenweit Variablen festgelegt werden, deren Werte die Anwender während des Rollouts festlegen können. Diese können dann in Konfigurationen genutzt werden.

2.7.3 Geräteregeln

Die Geräteregeln ermöglichen das mandantenweite Einstellen von Workflows für iOS, Android und Windows Phone 8 Geräte. Für die selektierten Bedingungen können Aktionen wie Benachrichtigungen und das Entfernen des Geräts aus der Kontrolle des MDMs definiert festgelegt werden.

2.7.4 Einstellungen für Benutzer

In diesem Bereich können Kennwortrichtlinien für die pureMDM Benutzer definiert werden.

2.7.5 E-Mail-Vorlagen

Die vorhandenen E-Mail-Vorlagen können in diesem Bereich inhaltlich frei sowie Ihrer Business-Logik entsprechend, angepasst werden. Verwendet werden die Vorlagen in Verbindung mit den entsprechenden Gerätekonfigurationen (siehe Abschnitt 2.3.3), wo sie optional aktiviert werden können. In den E-Mail-Vorlagen sind Variablen einsetzbar. Die Liste der Variablen ist abhängig vom Verwendungszweck der Vorlage. Sie werden in der Oberfläche dargestellt.

Es gibt drei Arten von Variablen:

1. Attribute des Objektes für die die E-Mail verschickt wird, z.B. der Name des Gerätes oder der Name des Benutzers des Gerätes
2. Ergebnisvariablen der Aktion, für welche die E-Mail verschickt wird.
3. Globale Variablen die in den Einstellungen gesetzt wurden.

Variablen beginnen und enden immer mit einem Prozent-Zeichen. Unbekannte Variablennamen werden ohne Änderung ausgegeben.

Für alle E-Mail-Vorlagen sind Vorschlagswerte vorhanden. E-Mails die an Benutzer verschickt werden sind in mehreren Sprachen vorhanden, Emails an einen Administrator nur in einer. Welche E-Mail-Vorlage für den Versand an den Benutzer verwendet wird, entscheidet die Spracheinstellung des Benutzers.

2.7.6 Nachrichtenvorlagen

Mit den Nachrichten-Vorlagen wird Ihnen die Möglichkeit gegeben, schnell und unkompliziert Ihre Mitarbeiter im Unternehmen per Push-Nachricht oder

SMS über Neuigkeiten zu informieren. Nachrichten-Vorlagen können Sie frei erstellen, bearbeiten, benennen und speichern.

2.7.7 Dokumentenvorlagen

Die Geräte, an die eine Nachricht verschickt werden soll, können Sie in der Geräteliste selektieren (hier ist Gruppenbildung durch das Selektieren mehrerer Geräte möglich). Daraufhin können das Versenden mit der Aktionsfolge „Aktionen/Sende SMS" oder „Aktion/Senden OS" und die Auswahl der Nachrichten-Vorlage erfolgen. Nachrichten können auch an gesamte Gerätegruppen verschickt werden. Dies erfolgt dann in der Symbolleiste des Gruppeneintrags über den Menüeintrag „Gerätebenachrichtigung/Sende SMS".

Mit den Dokumentenvorlagen wird Ihnen die Möglichkeit gegeben, pdf-Dokumente aus Geräten, Mitarbeitern oder Verträgen zu erstellen, z.B. für Ausgabebelege oder Rückgabebelege von Geräten, Datenschutz-vereinbarungen usw.

Das Bearbeitungsfenster besteht aus einer Arbeitsfläche rechts, einer Objektbibliothek links oben und einem Übersichtsfenster links unten. Zur Bearbeitung ziehen Sie aus der Objektbibliothek ein Objekt auf die Arbeitsfläche. Um ein Objekt zu bearbeiten markieren Sie es mit der linken Maustaste und öffnen Sie das Popup-Menü mit der rechten Maustaste, welches Ihnen weitere Bearbeitungsfunktionen zur Verfügung stellt. Für Text-objekte können innerhalb des Textes Variablen verwendet werden. Die gültigen Variablen werden im Bearbeitungsfenster angezeigt.

2.8 Auswertungen

Im Bereich Auswertungen können eine Vielzahl von Berichten erstellt werden. Dies geschieht durch einfache Auswahl des gewünschten Eintrags, woraufhin die Auswertung eingeblendet wird.

Es können z.B. Auswertungen nach den verschiedenen Geräteklassen, Typen, oder nach der installierten Software erstellt werden. Eine Filterung ist jederzeit per Drag & Drop der Spaltenüberschriften in die darüber liegende Zeile möglich. Sie können den Bericht anschließend zwecks Weiterverarbeitung exportieren.

Folgende Auswertungen stehen zum Abruf bereit:

- Geräte

- Geräteinventur
  - Android
    - Android
    - Bluetooth
    - Gerät
    - Speicher
    - Telefon
  - iOS
    - Afaria
    - Bluetooth
    - Zertifikate
    - Gerät
    - Speicher
    - MS Exchange
    - Telefon
    - Provisionierungsprofile
    - Payloads
    - Restriktionen
    - Sicherheit
    - WiFi
  - Windows Mobile Professional
    - Bluetooth
    - Benutzerdefinierte Daten
    - Gerät
    - RDA (Remote Data Access)
    - Speicher
    - Telefon
    - Externe Geräte
    - WiFi
- Geräte pro Typ
- Geräte pro Gruppe
- Alle Geräte
- Geräteprotokoll
- Geräte ohne Benutzerzuordnung

- Software
  - Installierte Software
  - Nicht installierte App-Empfehlungen
  - Software ohne App-Empfehlung

- Mitarbeiter
    - Geräte gesperrter Mitarbeiter
    - Geräte zukünftig gesperrter Mitarbeiter
    - Benutzerzertifikate
- Verträge
    - Kündbare Verträge

3 DIE WICHTIGSTEN ARBEITSFOLGEN / FAQS

3.1 Wie wird die pureMDM-Umgebung eingerichtet?

Nach der Inbetriebnahme Ihrer pureMDM-Umgebung ist diese mit den Daten Ihres Unternehmens (Abteilungen und Kostenstellen) sowie Ihrer Mitarbeiter zu füllen. Danach können Einträge für Tarife, Verträge (siehe Abschnitt 3.1.2.5), Gerätekonfigurationen und Gerätegruppen (siehe Abschnitt 3.5) sowie Software und Software-Kategorien (siehe Abschnitt 3.6) erstellt werden.

Die Anlage eines einzelnen Benutzers wird in Abschnitt 3.4.1 beschrieben. Bei der Anlage und Pflege von vielen Einträgen ist die Nutzung der Import-Funktion zu empfehlen. Diese unterstützt Excel- und CSV-Dateien, welche die nachfolgenden Punkte beschreiben. Optional besteht die Möglichkeit eine Schnittstelle zu Ihrem Active Directory herzustellen.

3.1.1 Vorbereiten der Import-Dateien

Die Import-Dateien können entweder im Excel-Dateiformat (.xls oder .xlsx) oder CSV-Dateiformat bereitgestellt werden.

3.1.1.1 Mitarbeiterdaten

Um Mitarbeiterdaten importieren zu können, benötigt pureMDM eine bestimmte Formatierung der Excel-Tabelle oder CSV-Datei. Die erste Zeile muss als Spaltenüberschriften die unten stehenden Einträge in folgender Reihenfolge aufweisen:

- Nachname
- Vorname
- Benutzername*
- Personalnummer
- E-Mail
- Abteilung
- Eintrittsdatum
- Austrittsdatum
- Standardsprache
- Standard Gerätegruppe
- Standardkostenstelle

* Pflichtfelder

Excel-Tabellen und CSV-Dateien in dem benötigten Format können auf folgendem Weg direkt in pureMDM generiert werden:

1. Wechseln Sie zur Mitarbeiterliste.
2. Klicken Sie auf die Schaltfläche „Export“ und wählen Sie das gewünschte Dateiformat.
3. Wählen Sie den Speicherplatz der Datei oder öffnen Sie diese, um sie direkt bearbeiten zu können.
4. Die Tabelle kann jetzt mit den Mitarbeiterdaten gefüllt werden.

Pflichtfelder sind „Nachname“, „Vorname“, „Benutzername“ und „E-Mail“. Die restlichen Spalten können bei Bedarf gefüllt werden. Diese sollten Sie vor dem Datenimport berücksichtigen.

3.1.1.2 Kostenstellen

Auch hier benötigt pureMDM eine korrekte Formatierung der Tabelle mit folgenden Spaltenüberschriften:

- Name*
- Beschreibung
- Verantwortlicher
- Beginn
- Ende

* Pflichtfeld

Eine Tabelle in diesem Format können Sie auf dem gleichem Weg erstellen wie schon für die Mitarbeiterdaten beschrieben:

1. Wechseln Sie zu der Liste der Kostenstellen.
2. Klicken Sie auf die Schaltfläche „Export“ und wählen Sie das gewünschte Dateiformat.
3. Wählen Sie den Speicherplatz der Datei oder öffnen Sie diese, um sie direkt bearbeiten zu können.
4. Die Tabelle kann jetzt mit den Kostenstellendaten des Unternehmens gefüllt werden.

Zu füllendes Pflichtfeld ist hier nur „Name“.

3.1.1.3 Verträge

Die Spaltenüberschriften für die Vertragsdaten sind wie folgt:

- Nummer*



- Tarif*
- Datum*
- Beginn*
- Ende
- Bemerkung
- Ablage

Zu bemerken ist, dass die Einträge in der Spalte „Tarif" genau mit den Tarifnamen (Abschnitt 3.1.2.4) übereinstimmen müssen. Darüber hinaus kann die Option „Erlaube mehrere SIM-Karten" für jeden Vertrag erst nach dem Import definiert werden.

3.1.1.4 Geräte

Wenn ein optionales pureMDM Portal zum Rollout genutzt wird, so müssen Sie den Nutzern vor dem Rollout ihre Geräte zuweisen. Dies ist auch per Daten-Import möglich. Das Format ist wie folgt:

- Gerätename*
- Beschreibung
- Betriebssystem*
- IMEI
- Seriennr.
- Vertrag
- Mitarbeiter
- Gruppe
- Kostenstelle

*Pflichtfelder



3.1.2 Importieren bzw. Eintragen der Daten

3.1.2.1 Erster Import der Mitarbeiterdaten sowie der Kostenstellen

1. Wechseln Sie zur Mitarbeiterliste.

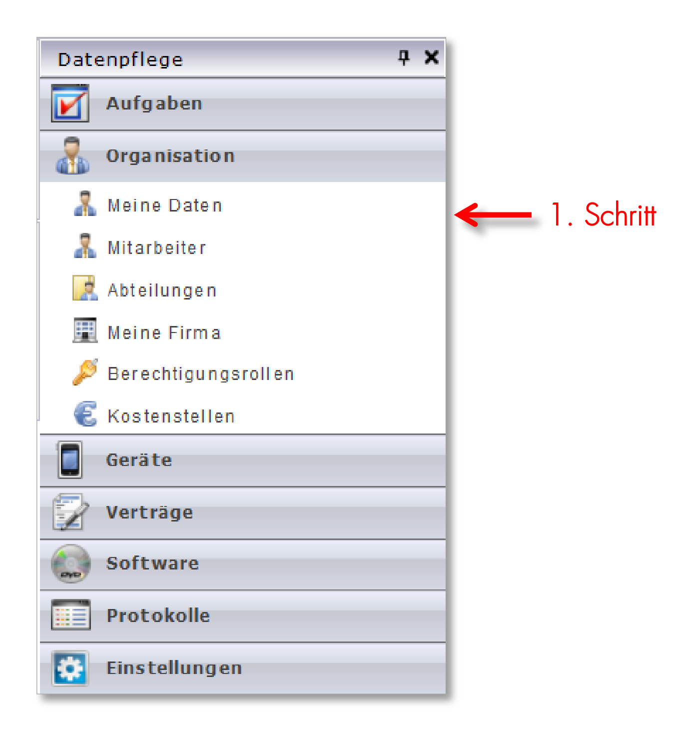


Abbildung 1 – Menü „Mitarbeiter“

2. Klicken Sie auf die Schaltfläche „Import“.

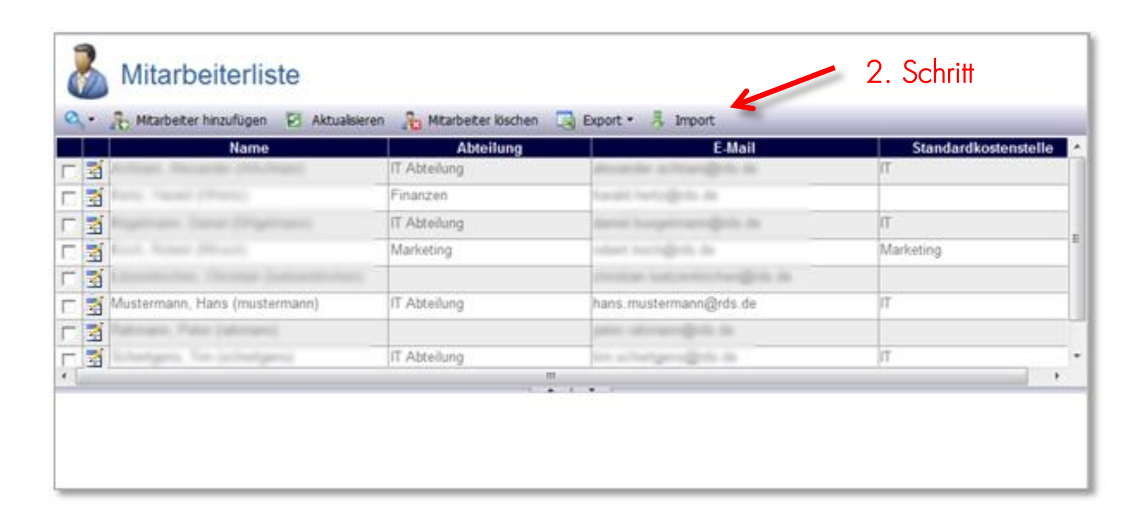


Abbildung 2 – Die Mitarbeiterliste

3. Wählen Sie über die Schaltfläche „Durchsuchen“ die unter Abschnitt 3.1.1.1 erstellte Datei.
4. Deselektieren Sie, wie in Abbildung 3 - Mitarbeiterimport gezeigt, alle optionalen Spaltenüberschriften.
5. Gehen Sie sicher, dass „Daten hinzufügen“ ausgewählt ist.
6. Klicken Sie auf die Schaltfläche Import, um den Vorgang abzuschließen.

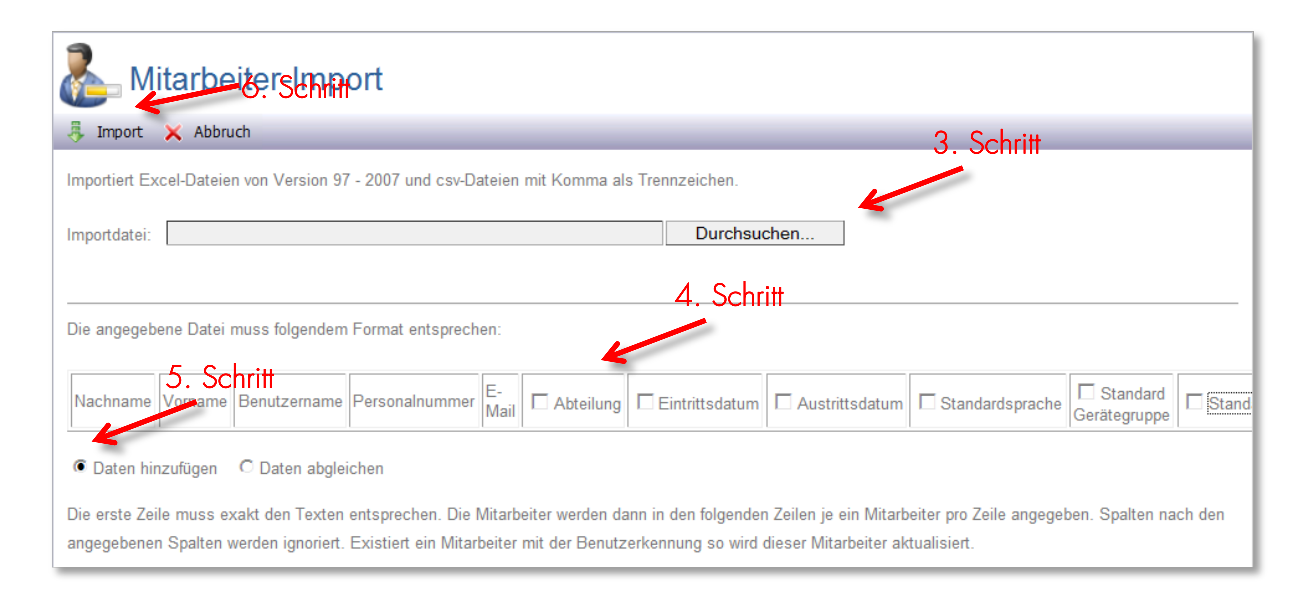


Abbildung 3 - Mitarbeiterimport

Für die Kostenstellen wird in gleicher Weise verfahren, außer dass es hier keine optionalen Spalten gibt.

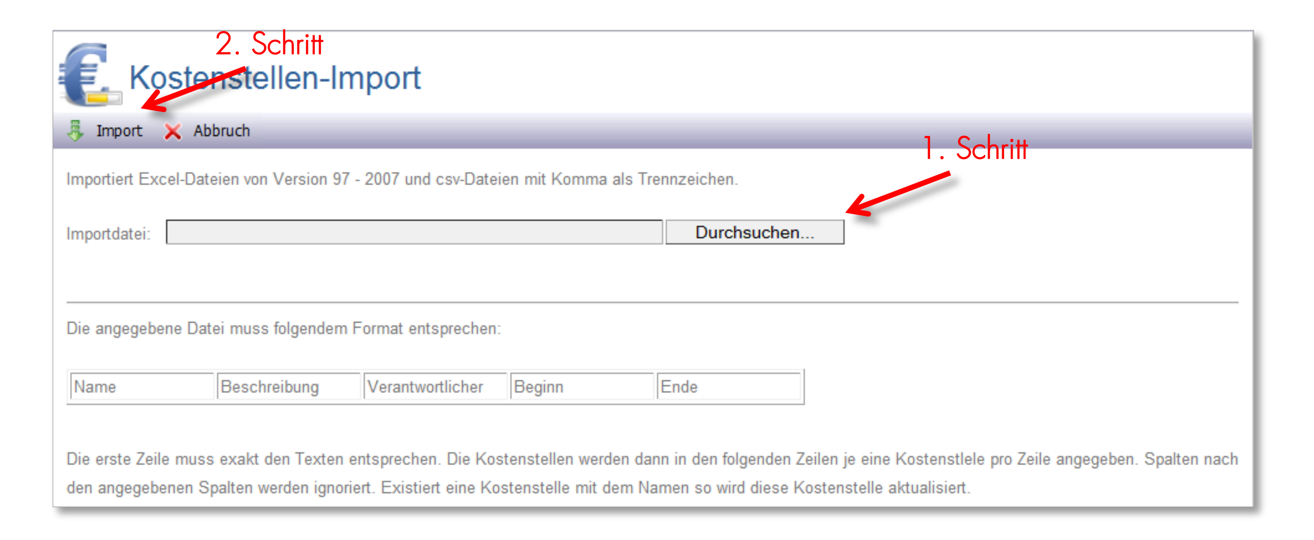


Abbildung 4 - Import der Kostenstellen

3.1.2.2 Anlegen der Abteilungen

Die Abteilungen müssen manuell angelegt werden. Hierzu gehen Sie bitte folgendermaßen vor:

1. Wechseln Sie zur Abteilungsliste.

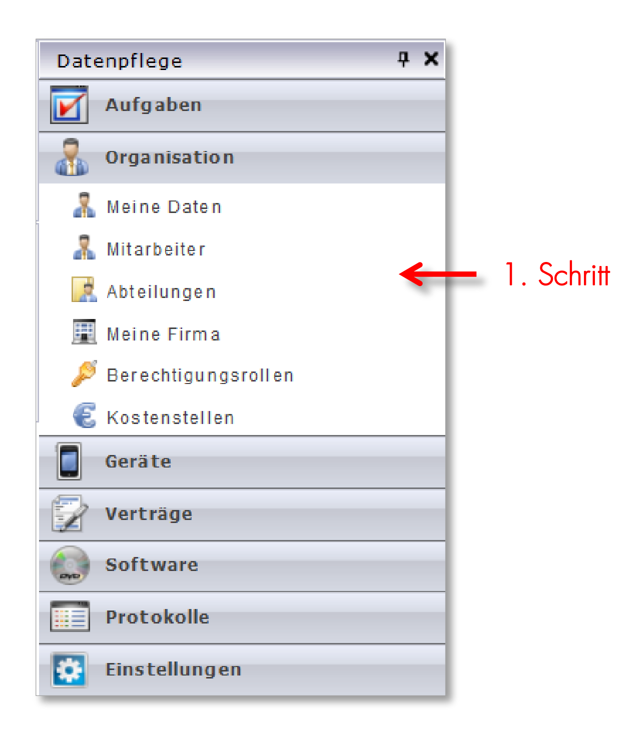


Abbildung 5 – Menüpunkt „Abteilungen"

2. Klicken Sie auf die Schaltfläche „Neu parallel". Wenn eine bereits angelegte Abteilung ausgewählt wurde, kann über die Schaltfläche „Neu untergeordnet" eine Unterabteilung angelegt werden.



Abbildung 6 - Das Anlegen von Abteilungen



3. Tragen Sie die Daten der Abteilung ein. Pflichtfeld ist hier „Name". Wenn die Mitarbeiterdaten und Kostenstellendaten (siehe Abschnitt 3.1.2.1) sowie die Gerätegruppendaten (siehe Abschnitt 3.5) vorhanden sind, können Sie die Felder „Leiter", „Standardkostenstelle" und „Standard Gerätegruppe" füllen.
4. Klicken Sie auf die Schaltfläche „Speichern".

3.1.2.3 Abgleich der Mitarbeiterdaten

Nach dem Anlegen der Abteilungen und Kostenstellen können diese Daten auch den Mitarbeitern zugewiesen werden. Wenn diese Daten schon in der Mitarbeiter-Import-Datei vorhanden sind, können Sie diese zum Datenabgleich nutzen:

1. Wechseln Sie zur Mitarbeiterliste.
2. Klicken Sie auf die Schaltfläche „Import".
3. Wählen Sie über die Schaltfläche „Durchsuchen" die unter 3.1.1.1 erstellte Datei.
4. Sie können jetzt alle Spaltenüberschriften selektieren, da die nötigen Datenbankeinträge jetzt vorhanden sind.
5. Wählen Sie „Daten abgleichen".
6. Klicken Sie auf die Schaltfläche „Import".

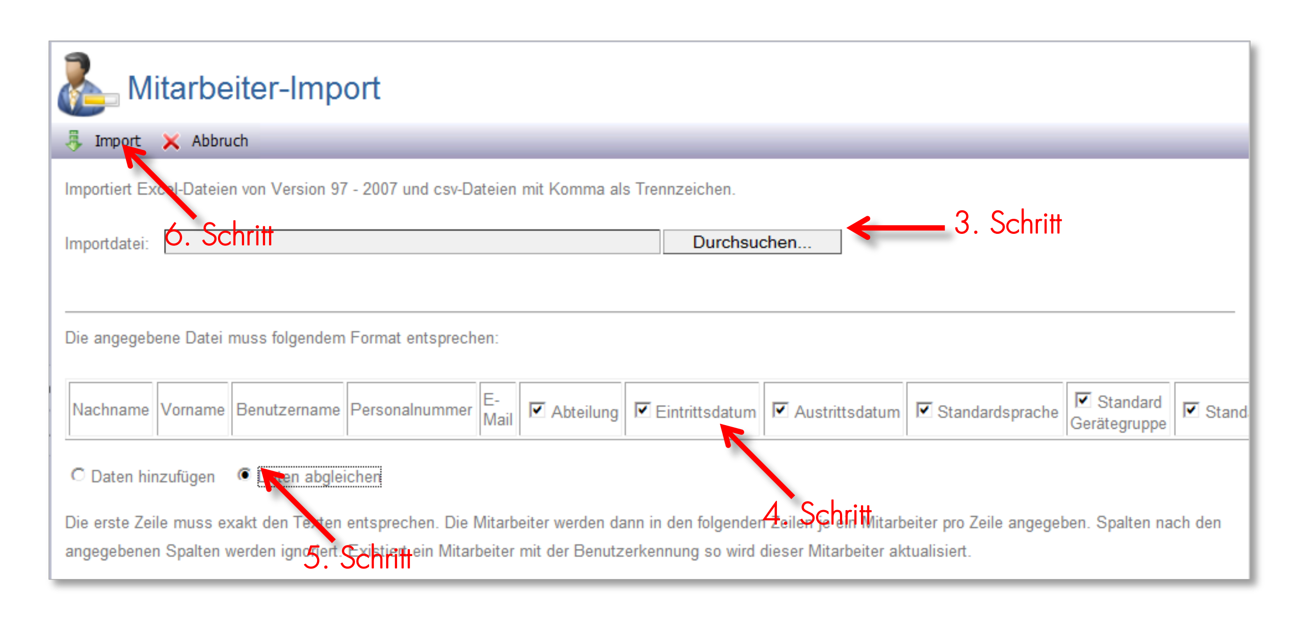


Abbildung 7 - Der Mitarbeiter-Import

3.1.2.4 Anlegen der Tarife

Einträge für Tarife müssen manuell angelegt werden.

1. Wechseln Sie zur Seite „Tarife".

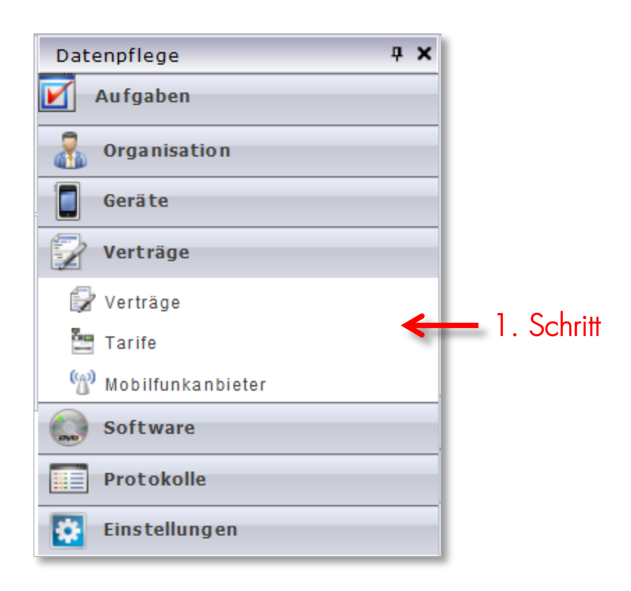


Abbildung 8 – Menüpunkt „Tarife"

2. Klicken Sie auf die Schaltfläche „Tarif hinzufügen".
3. Füllen Sie die Felder aus und klicken Sie auf die Schaltfläche „Speichern".

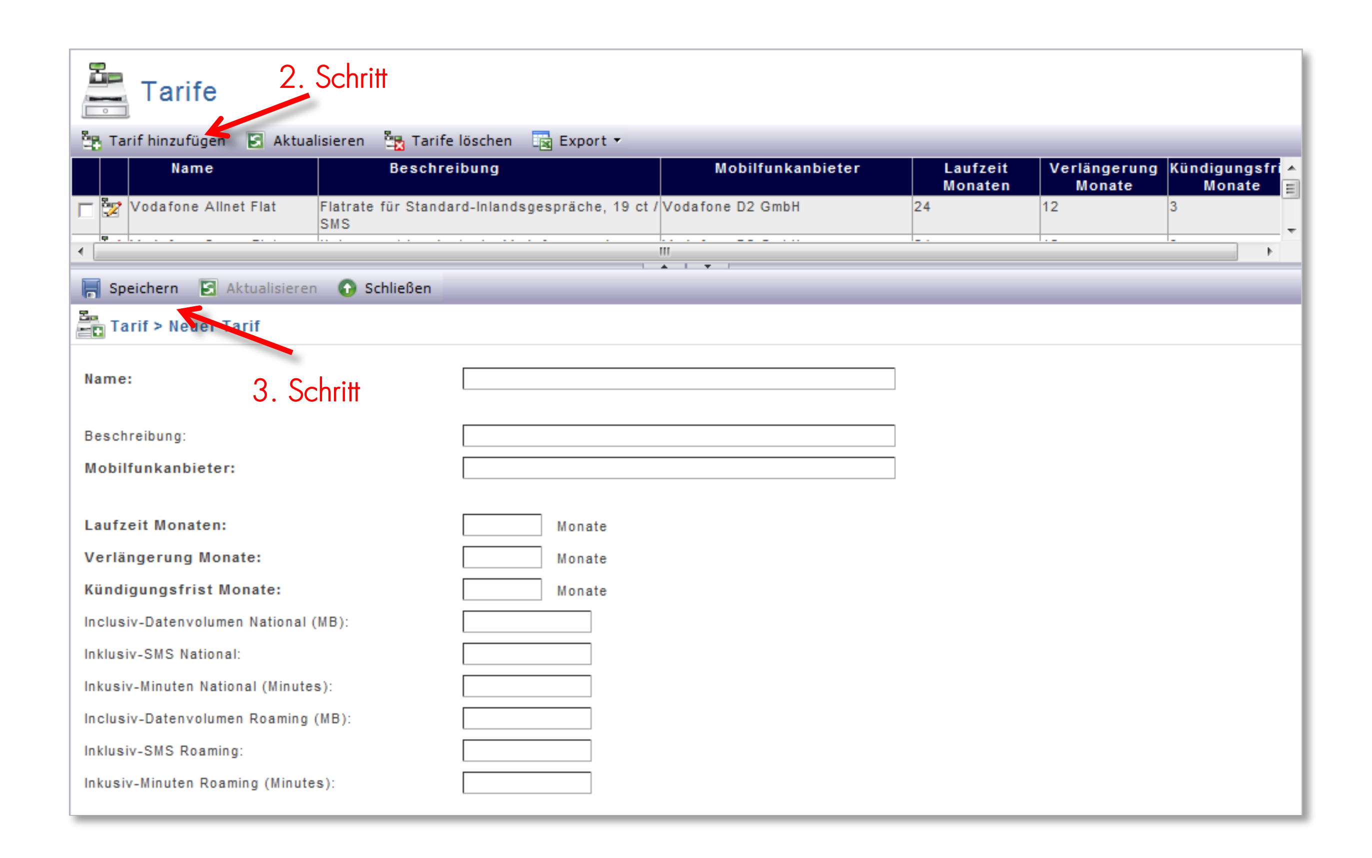


Abbildung 9 - Das Anlegen von Tarifen

3.1.2.5 Importieren der Vertragsdaten

1. Wechseln Sie zu der Vertragsliste.

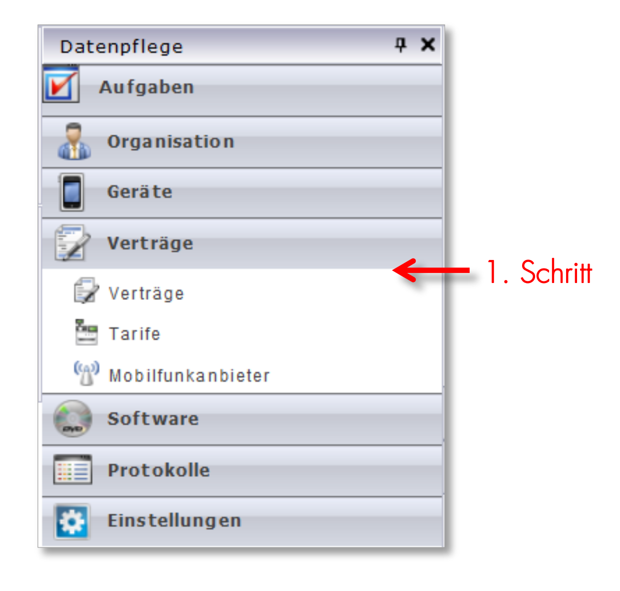


Abbildung 10 – Menüpunkt „Verträge“



2. Klicken Sie auf die Schaltfläche „Import".
3. Klicken Sie auf „Durchsuchen…" und wählen Sie die unter Abschnitt 3.1.1.3 erstellte Datei.
4. Wählen Sie „Daten hinzufügen" und klicken Sie auf die Schaltfläche „Import".



Abbildung 11 – Der Vertrags-Import

5. Aktivieren Sie für die relevanten Verträge ggf. die Option „Erlaube mehrere SIM-Karten" und tragen Sie die SIM-Kartennummern ein.

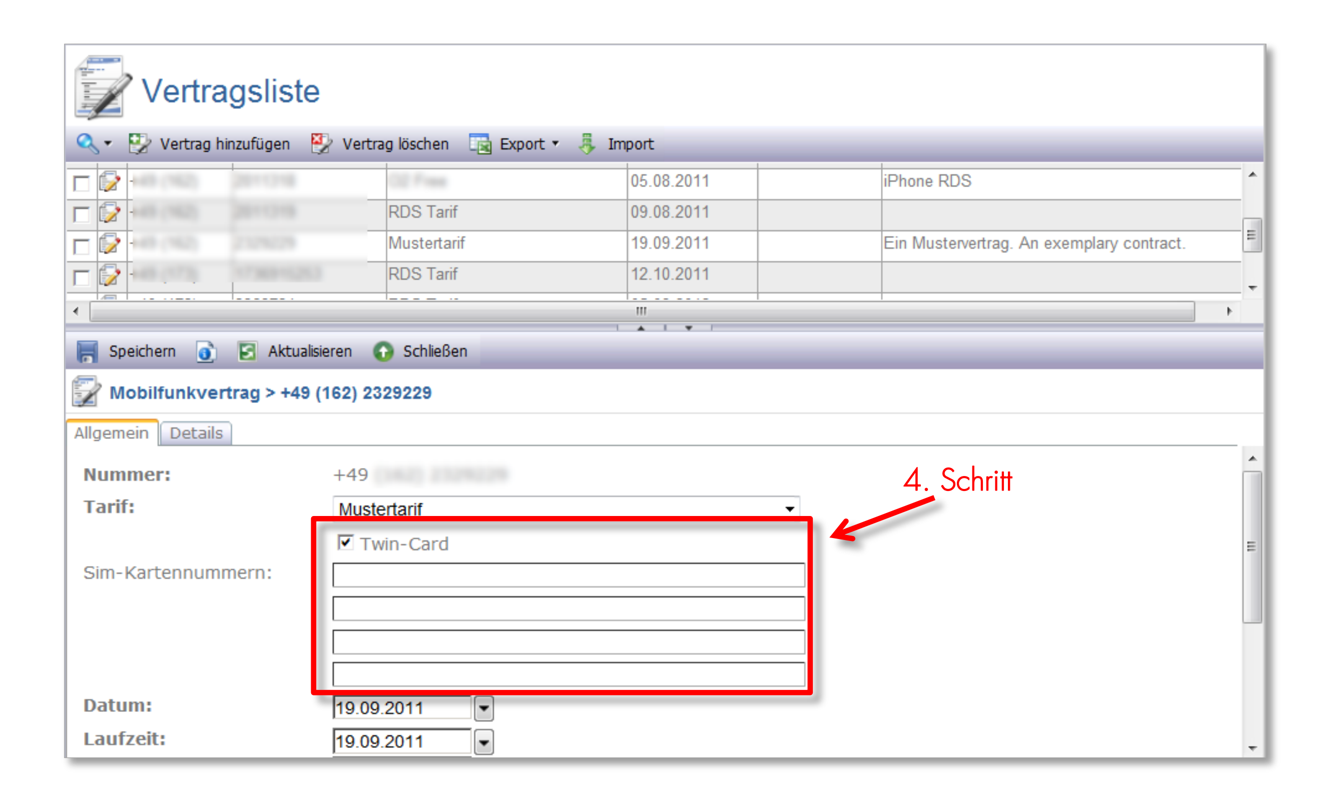


Abbildung 12 – Felder für SIM-Kartenummern

3.1.2.6 Importieren der Gerätedaten

1. Wechseln Sie zur Geräteliste und klicken Sie die Schaltfläche „Import".
2. Klicken Sie auf „Durchsuchen…" und wählen Sie die Import-Datei (3.1.1.4) aus.
3. Klicken Sie auf die Schaltfläche „Import".

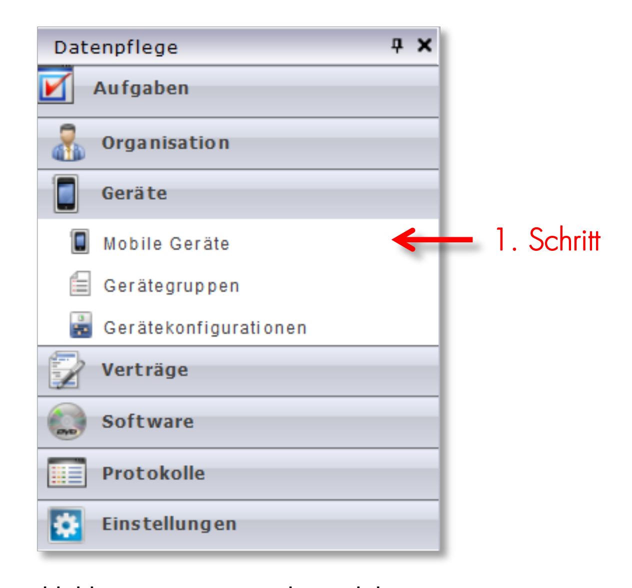


Abbildung 13 – Menüpunkt „Mobile Geräte"



Abbildung 14 - Geräte-Import

3.2 Wie wird ein mobiles Gerät ausgerollt?

In den folgenden Schritten wird das Einbinden eines Gerätes über die Web-Oberfläche des pureMDM dargestellt.

3.2.1 Rollout mit einem Registrierungscode

Diese Methode benötigt einen bestehenden Eintrag in der Geräteliste sowie einen bereits installierten Afaria Client auf dem mobilen Gerät selbst.

1. Wechseln Sie zur Geräteliste. Öffnen Sie den Eintrag des Gerätes und klicken Sie auf die Schaltfläche „Gerätebenachrichtigung“, gefolgt von „Generiere Registrierungscode“. Alternativ kann dieser auch direkt an den Anwender per E-Mail gesendet werden („Gerätebenachrichtigung“, gefolgt von „Sende Registrierungscode an Benutzer“).

Geräteliste

Gerät hinzufügen | Aktualisieren | Lösche markierte Geräte | Aktionen | Export | Import

iPhone Mustermann

1. Schritt

Speichern | Aktualisieren | Aktionen | Gerätebenachrichtigung | Sicherheit | Schließen

Mobiles Gerät > iPhone Mustermann

Allgemein | Geräteinformationen | Software | Protokoll

Sende Einstellungen
Binde Gerät ein
Konfiguriere Afaria Client
Generiere Registrierungscode
Sende Registrierungscode an Benutzeremail
Sende Registrierungscode als SMS
Entferne Registrierungscode

2. Schritt

3. Schritt

Gerätedaten

Gerätename: iPhone Mustermann
Beschreibung:
Eigentum: Unternehmen / Privat / Unbekannt
Modell:
Betriebssystem: iOS
Vertrag:
IMEI:
Seriennr.:
Mitarbeiter: Mustermann, Max (afaria\MMustermann)
Kostenstelle:
Gerätebenachrichtigung: SMS / Email

Abbildung 15 - Registrierungscode generieren

2. Das System generiert einen Registrierungscode und zeigt diesen an.

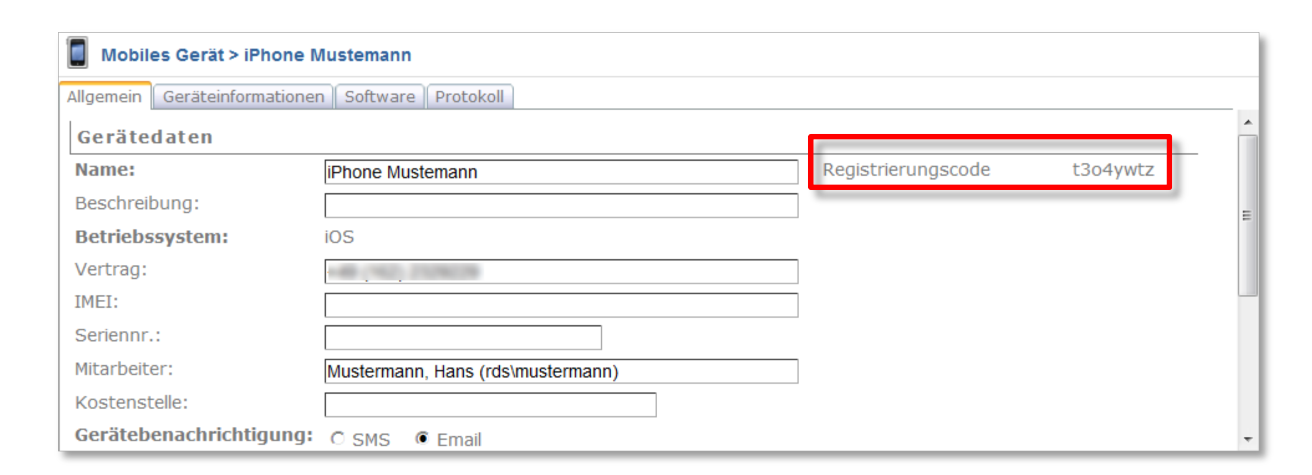


Abbildung 16 - Anzeige des Registrierungscodes

3.2.1.1 iOS

3. Der Nutzer kann auf seinem Gerät den Afaria Client starten. Dieser fragt beim Erst-Start den Registrierungscode ab:

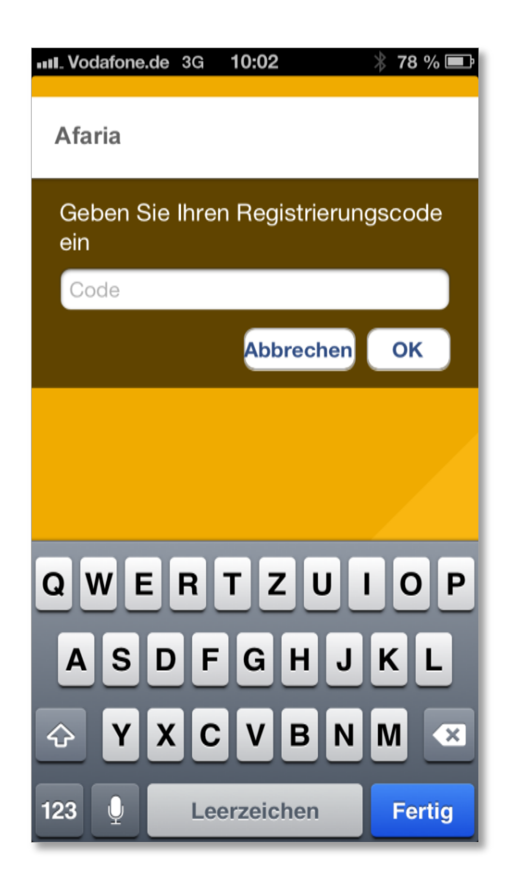


Abbildung 17 - Eingabe des Registrierungscodes

4. Eingabe der Authentifizierungsdaten (Hängt von der Konfiguration des Rolloutvorgangs ab)

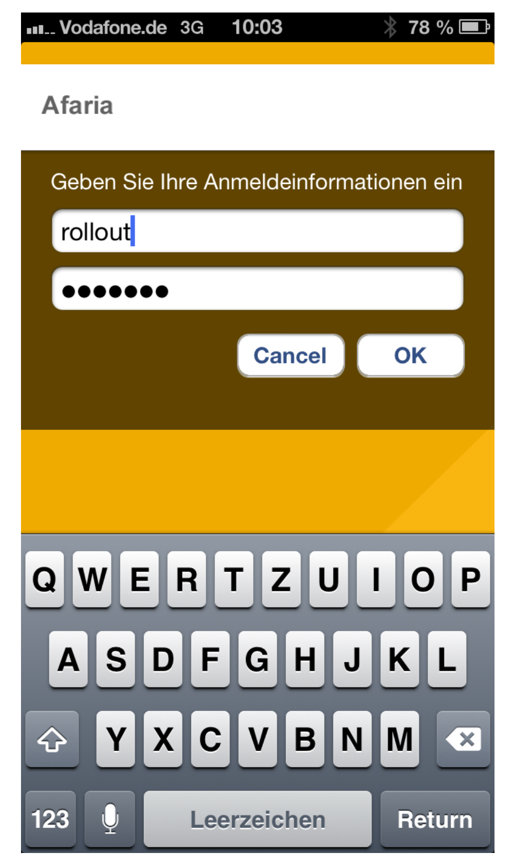


Abbildung 18 - Gerät ausrollen - Anmeldeinformationen eingeben

5. Auf dem Gerät wird eine Routine für die Profilinstallation ausgeführt. Bitte das Feld „Installieren“ aktivieren.

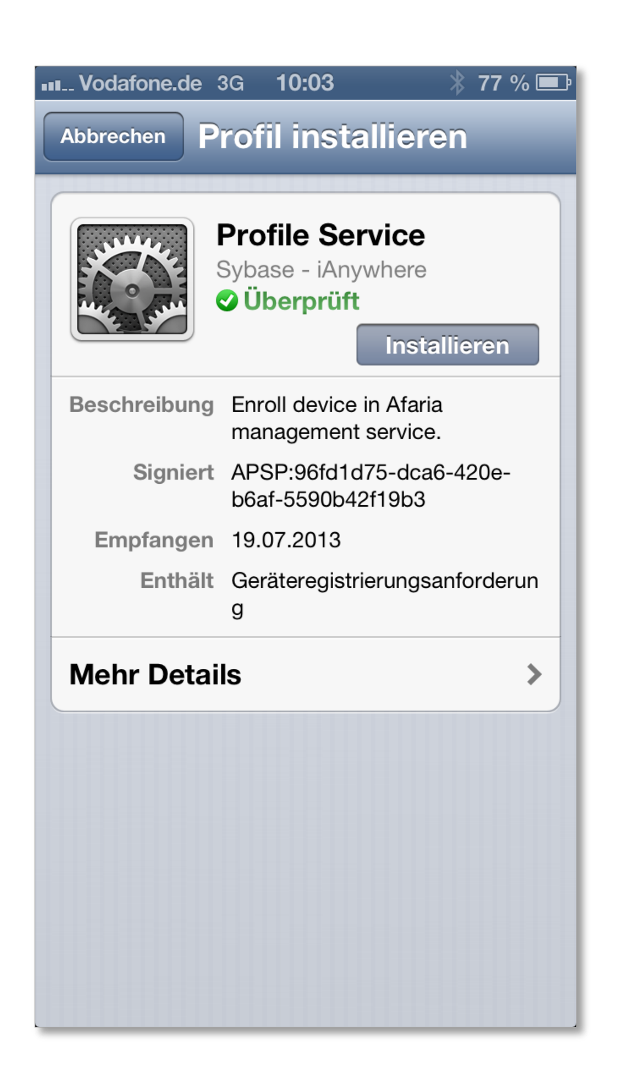


Abbildung 19 - Gerät ausrollen - Profil installieren aktivieren

6. Bestätigung des nicht überprüften Profils durch aktivieren des Feldes „Installieren". Dadurch wird auf dem Gerät ein Profil installiert, womit die Verwaltung über pureMDM ermöglicht wird.



Abbildung 20 - Gerät ausrollen - Profil bestätigen

7. Der Benutzer muss, falls bereits vorhanden, sein Geräte-Passwort eingeben.



Abbildung 21 - Gerät ausrollen – Code

8. Das Profil wird installiert. Der folgende Screenshot zeigt die automatische Installation.



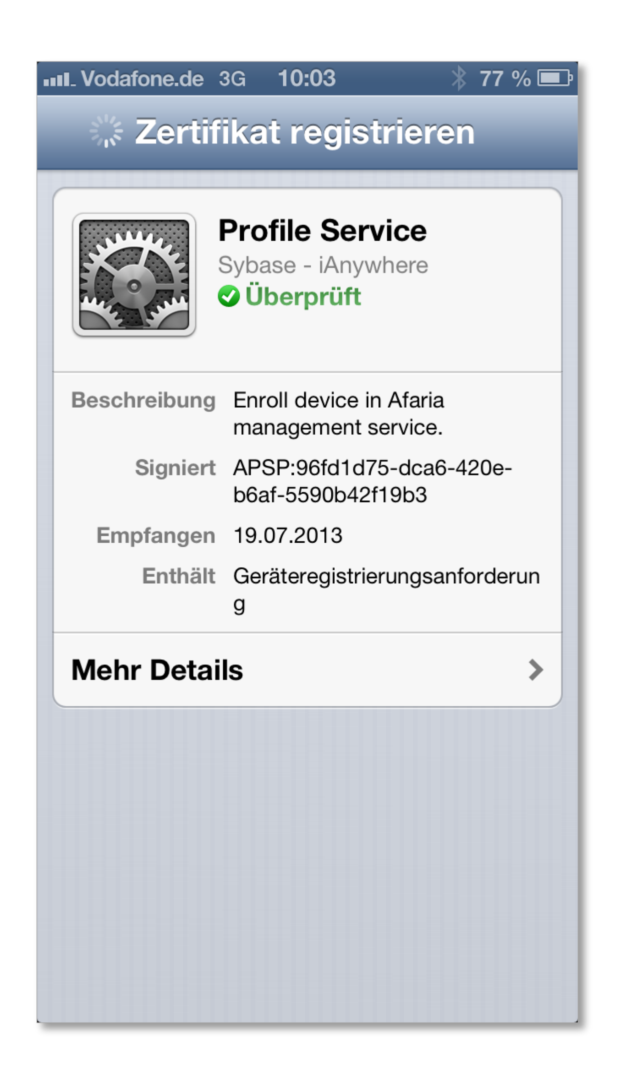


Abbildung 22 - Gerät ausrollen - Installation des Profils

9. Profil installieren: hier muss der Nutzer das Feld „Installieren" aktivieren.



Abbildung 23 - Gerät ausrollen - Installation des Profils 2

10. Das Profil wurde installiert und das Fenster kann durch Aktivierung des Feldes „Fertig" geschlossen werden. Das Gerät ist nun fertig ausgerollt und kann mit pureMDM vollständig administriert werden. Unter Umständen wird auf dem Gerät die letzte geöffnete Webseite angezeigt.



Abbildung 24 - Gerät ausrollen - Installation des Profils fertiggestellt

3.2.1.2 Android

3. Der Nutzer muss auf seinem Gerät den Afaria Client starten und die Geräteadministratorabfrage bestätigen.

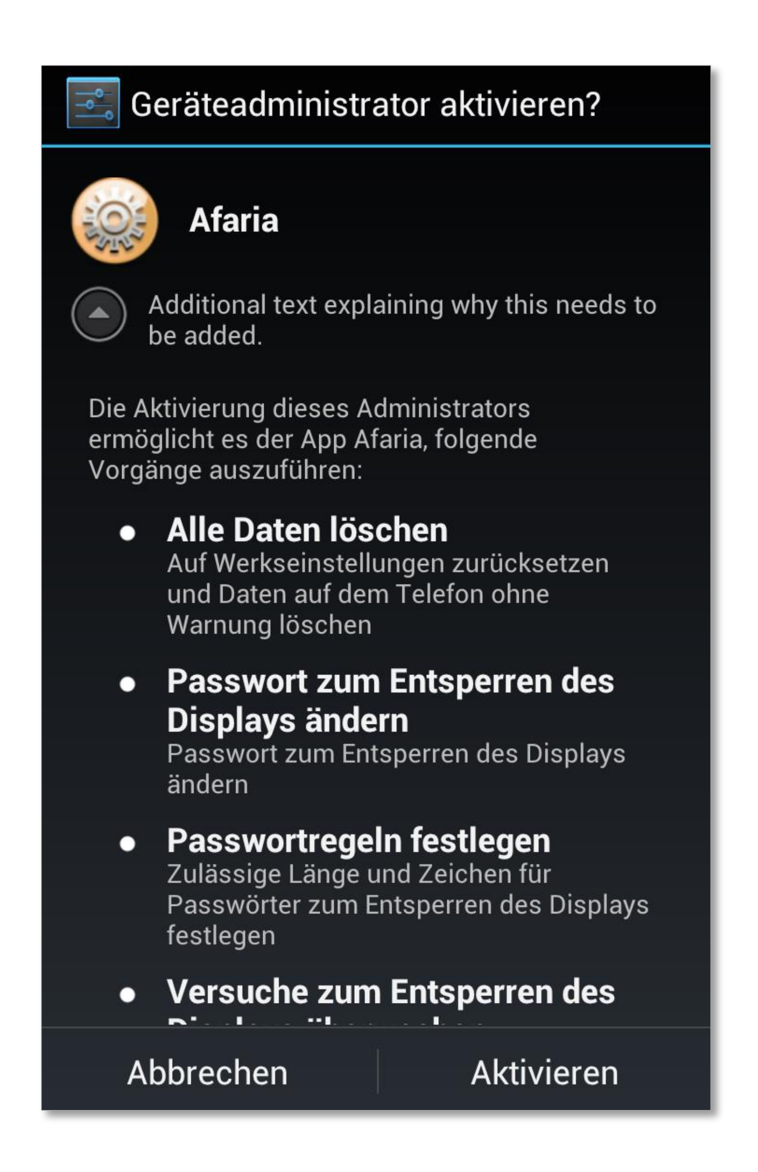


Abbildung 25 - Geräteadministratorabfrage

Der Client fragt daraufhin den Registrierungscode ab:



Abbildung 26 – Registrierungscode

11. Geben Sie den Registrierungscode in der Afaria App ein und bestätigen Sie mit „Fertig". Das Gerät verbindet sich anschließend selbstständig mit der Management Umgebung.



Abbildung 27 – Verbindung mit pureMDM

Bei Samsung Galaxy Geräten wird nach diesem Schritt eine weitere Komponente von dem Afaria Server heruntergeladen. Deren Geräteadministrator muss zusätzlich aktiviert werden.

3.3 Wie werden Einstellungen oder Restriktionen an das mobile Gerät übertragen?

In den nächsten Schritten wird der Versand einer Konfiguration (in diesem Beispiel eine WLAN-Konfiguration) an das mobile Gerät dargestellt. Wechseln Sie in pureMDM in den Bereich „Geräte/Mobile Geräte" und markieren das entsprechende Gerät zur Bearbeitung.

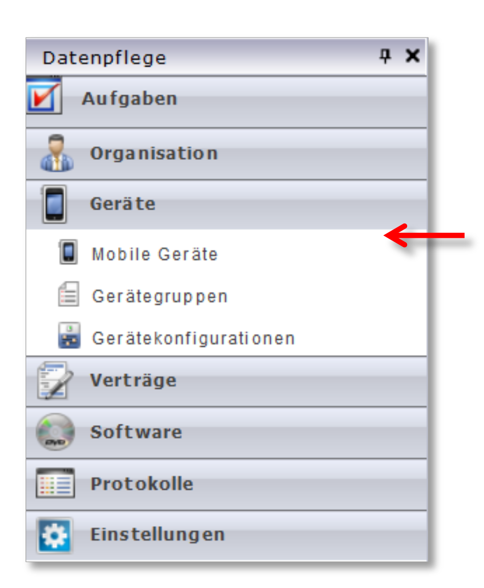


Abbildung 28 – Menüpunkt „Mobile Geräte“

1. Über das Feld „Gerätebenachrichtigung“ den Punkt „Sende Einstellungen“ auswählen.

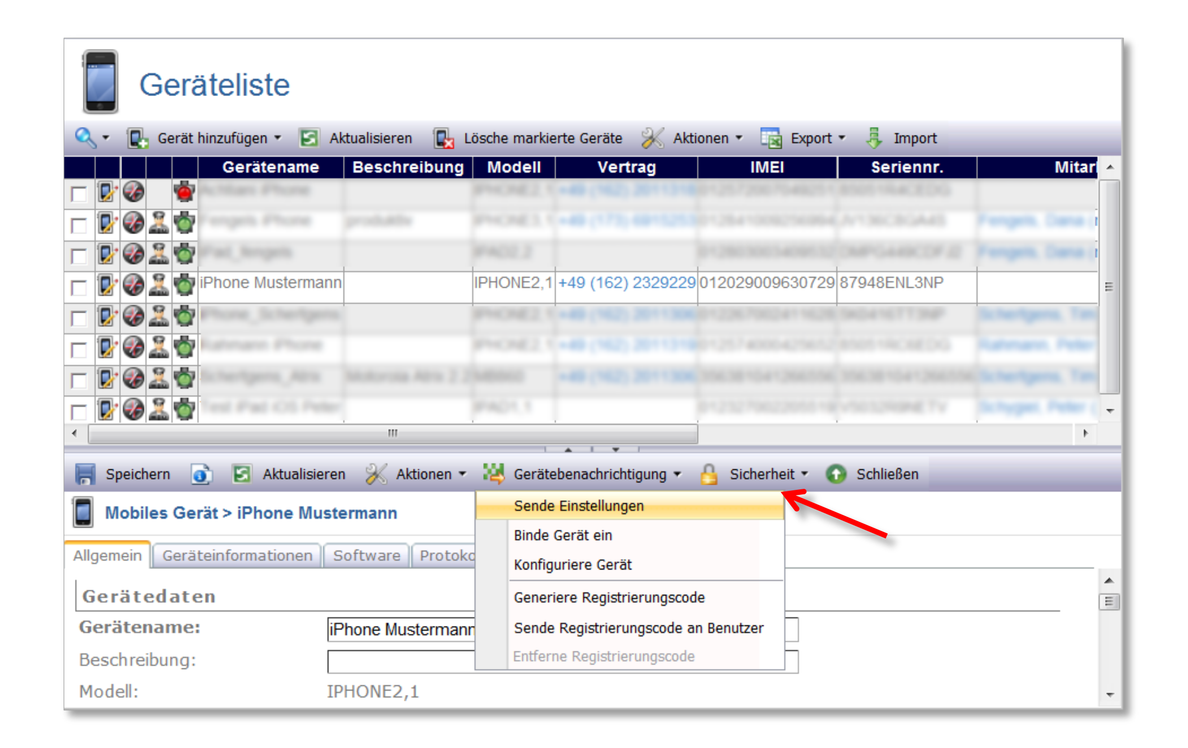


Abbildung 29 - Gerät ausrollen - Sende Einstellungen

Die Konfiguration wird an das mobile Gerät übertragen und erscheint unter den allgemeinen Einstellungen als zusätzliches Profil.



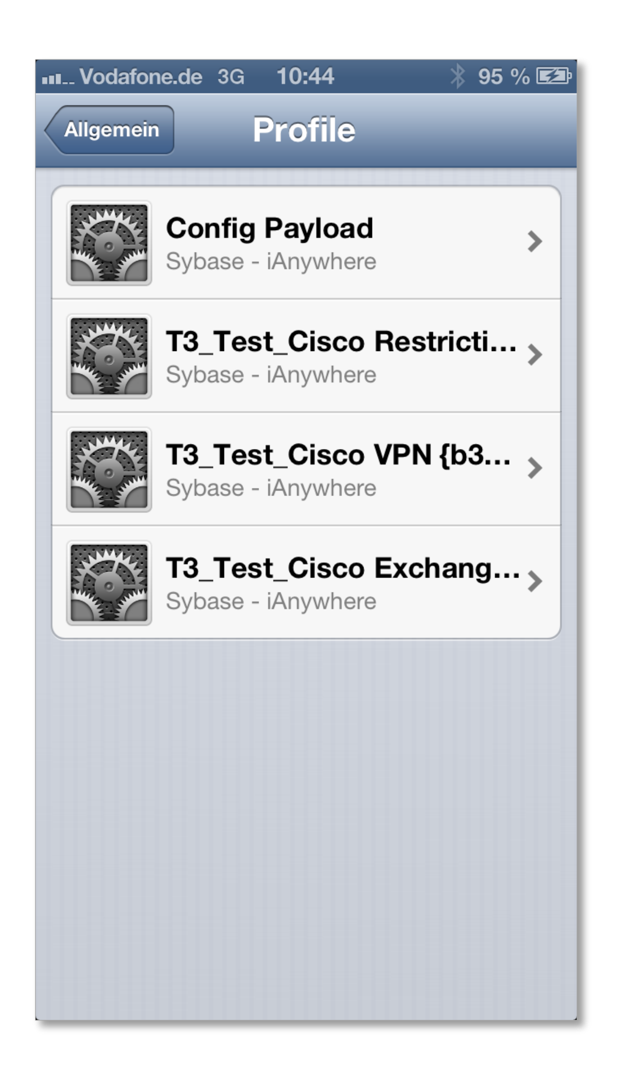


Abbildung 30 - Gerät ausrollen - Profil ist installiert 1

3.4 Wie kann ein Benutzer selbst das mobile Gerät in pureMDM einbinden?

Mit pureMDM und dem Self-Service ist ein Ausrollen und Einbinden des Gerätes – durch den Nutzer – innerhalb kurzer Zeit möglich. Der Self-Service stellt den Nutzern zwei Rollout-Methoden zur Verfügung.

Die erste Methode wird über ein optionales pureMDM Portal ausgeführt und wird in der entsprechenden Dokumentation beschrieben. Die zweite Methode beinhaltet den Aufruf der pureMDM Web-Oberfläche mit einem mobilen Gerät. pureMDM erkennt von welchem Gerät der Aufruf stattfindet und stellt eine angepasste Mobile-Seite zur Verfügung, über welche der Rollout ausgeführt werden kann.

Der Nutzer muss in pureMDM angelegt und konfiguriert sein. Jeder neue Benutzer bekommt automatisch die Berechtigungsrolle „Public“. Ihm sollte eine passende Benutzer-Rolle zugewiesen werden, die es ihm erlaubt sein eigenes Gerät ins zentrale Management aufzunehmen. Im Anschluss öffnet der Nutzer auf dem mobilen Gerät die pureMDM-Web-Oberfläche und wird innerhalb kurzer Zeit durch den Rollout geführt.

Danach ist keine abschließende administrative Tätigkeit mehr notwendig. Das Gerät ist vollständig eingebunden und konfiguriert.

3.4.1 Was muss ich in pureMDM als Vorbereitung tun?

In pureMDM muss ein Benutzer angelegt und der richtigen Benutzer-Rolle zugewiesen werden.

Folgende Schritte sind notwendig:

1. Anlegen des Benutzers, welcher z.B. das iPad selbst ausrollt. In den Bereich Organisation/Mitarbeiter wechseln.

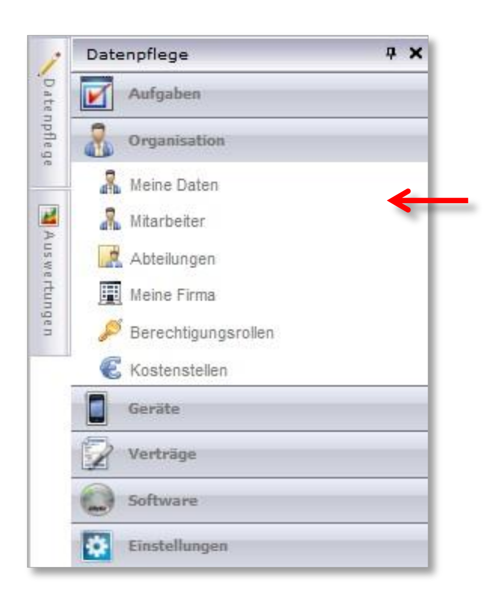


Abbildung 31 – Menüpunkt „Mitarbeiter“

2. Den Punkt „Mitarbeiter hinzufügen“ aktivieren, die Daten eingeben und „Speichern“ wählen.

Mitarbeiterliste

Mitarbeiter hinzufügen | Aktualisieren | Mitarbeiter löschen | Export | Import

1. Schritt

Name	Abteilung	E-Mail	Standardkostenstelle
[illegible]	IT Abteilung	[illegible]	IT
[illegible]	Finanzen	[illegible]	
[illegible]	IT Abteilung	[illegible]	IT
[illegible]	Marketing	[illegible]	Marketing
[illegible]		[illegible]	
Mustermann, Hans (mustermann)	IT Abteilung	hans.mustermann@rds.de	IT
[illegible]		[illegible]	
[illegible]	IT Abteilung	[illegible]	IT

3. Schritt

Speichern | Aktualisieren | Kennwort ändern | Schließen

2. Schritt

Mitarbeiter > Neuer Mitarbeiter

Mitarbeiterdaten | Berechtigungen

Vorname:
Nachname:
Benutzername:
☐ Technischer Benutzer
Personalnummer:
Abteilung:
E-Mail:
Eintrittsdatum: 21.09.2011
Austrittsdatum:
Standardsprache: German (Germany)
Standardkostenstelle:
Standard Gerätegruppe:

Abbildung 32 - Anlage des Benutzers

3. Einmaliges Ändern der Berechtigungsrolle „Public". Wechseln Sie bitte in den Bereich Organisation/Berechtigungsrollen. Bearbeiten Sie die Rolle „Public", setzen Sie die im Screenshot markierten Haken bei „Eigenes Gerät" und aktivieren das Feld „Speichern".

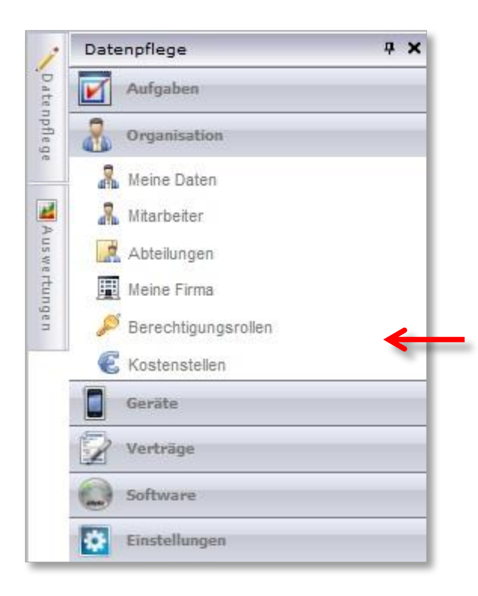


Abbildung 33 – Menüpunkt „Berechtigungsrollen"

Berechtigungsrollen

Rolle hinzufügen | Selektierte Rolle(n) löschen

		Name	
☐		Administrator	Admin
☐		Musterrolle	
☐		Public	Jeder
☐		Rolle IT-Department	
☐		User Rolle 1	

Speichern | Aktualisieren | Schließen

Berechtigungsrolle > Public

Meine Mitarbeiterdaten
- Sperre mein Gerät
- Entsperre mein Gerät
- Daten aus meinem Gerät löschen
- Entferne mein Gerät aus Kontrolle

Berechtigungsrollen

Geräte
- Provision Device
- Sende Einstellungen
- Konfiguriere Gerät
- Sperre Gerät
- Entsperre Gerät
- Daten aus Gerät löschen
- Entferne aus Kontrolle
- Eigenes Gerät ☑ ☑
- SMS senden

Verträge

Abbildung 34 - Ändern der Rolle "Public"

4. Sie teilen dem Benutzer das Passwort mit, indem Sie in der Mitarbeiterliste auf den entsprechenden Benutzer wechseln und das Feld „Kennwort ändern" aktivieren. Dem Benutzer wird nach dem Bestätigen des Feldes „OK" eine E-Mail mit dem Kennwort gesendet.

Name	Abteilung	E-Mail	Standardkostenstelle
[illegible]	IT Abteilung	[illegible]	IT
[illegible]	Finanzen	[illegible]	
[illegible]	IT Abteilung	[illegible]	IT
[illegible]	Marketing	[illegible]	Marketing
[illegible]		[illegible]	
Mustermann, Hans (mustermann)	IT Abteilung	hans.mustermann@rds.de	IT
[illegible]		[illegible]	
[illegible]	IT Abteilung	[illegible]	IT

Abbildung 35 - Benutzer-Kennwort 1

5. Falls der Benutzer ein optionales pureMDM Portal zum Rollout nutzt, muss ihm ein Gerät zugewiesen werden. Wechseln Sie hierzu zur Geräteliste und klicken Sie wahlweise auf „Gerät hinzufügen", um ein einzelnes Gerät hinzuzufügen oder auf „Import", um die Import-Funktion zu nutzen, um mehrere vorher erfasste Geräte hinzuzufügen.

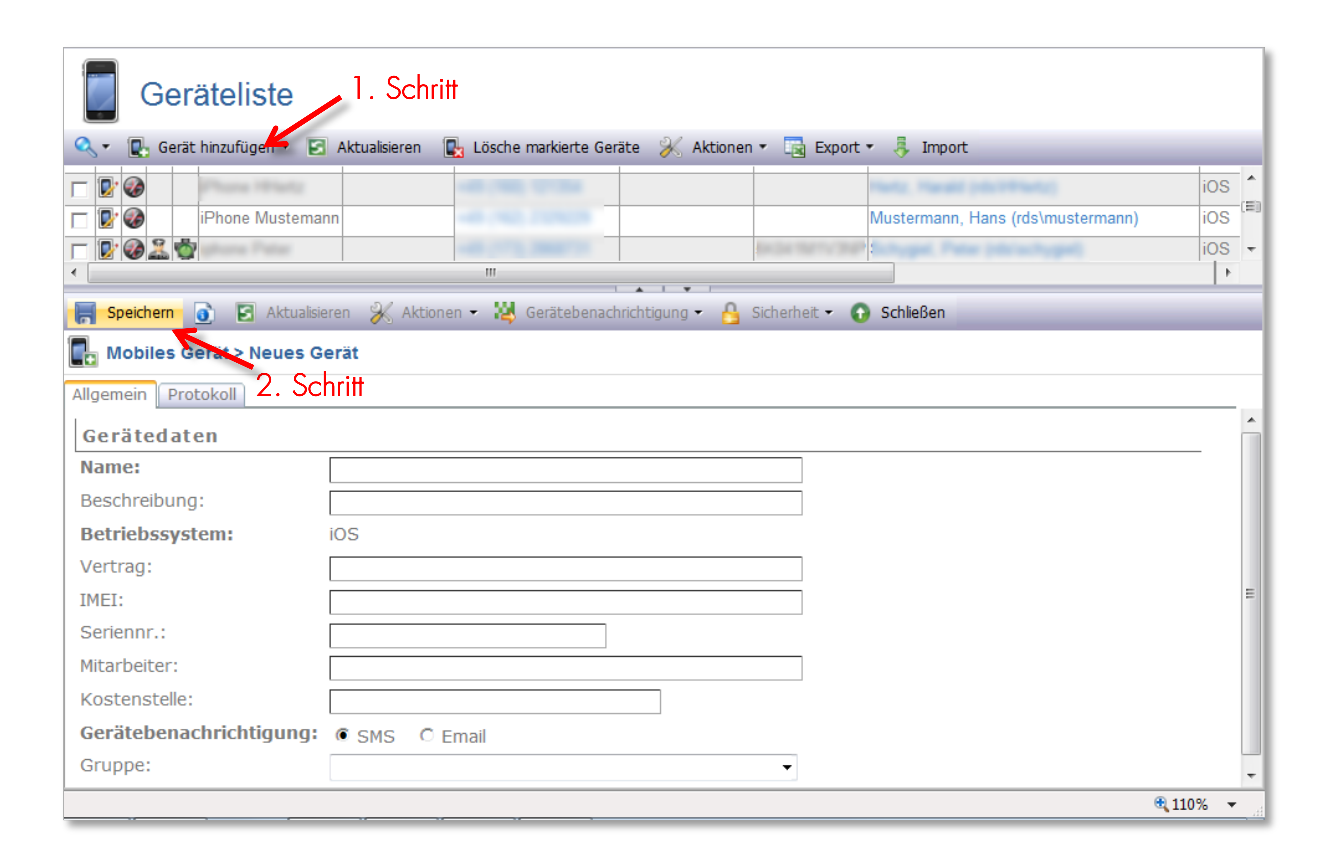


Abbildung 36 - Hinzufügen eines neuen Gerätes

Die Vorbereitungen in pureMDM sind somit abgeschlossen. Die abschließenden Schritte erledigt der Benutzer mit dem mobilen Gerät.

3.5 Wie werden Gerätekonfigurationen und Gerätegruppen erstellt und auf die mobilen Geräte verteilt?

In den Gerätegruppen werden eine oder mehrere Gerätekonfigurationen (z.B. Erzwingen eines Gerätekennworts oder Sperren bestimmter Funktionen) zu einer Gerätegruppe zusammengefasst. Es ist nicht möglich eine einzelne Gerätekonfiguration ohne die Aufnahme in eine Gerätegruppe an ein mobiles Gerät zu senden.

Die Verteilung kann entweder manuell, z.B. durch einen Administrator oder automatisiert vorgenommen werden. Für die automatisierten Vorgänge (Übertragung der Konfigurationen und Softwareüberwachung) müssen Sie Stundenanzahlen eintragen, in welchem Zeitintervall diese durchgeführt werden.

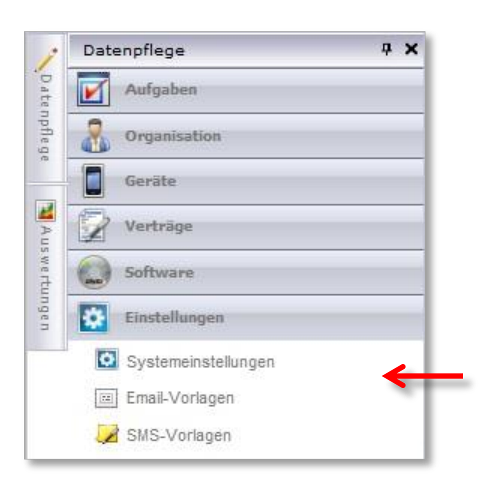


Abbildung 37 – Menüpunkt „Systemeisntellungen"



Abbildung 38 - Systemeinstellungen

3.5.1 Wie wird eine Gerätekonfiguration erstellt und in eine Gerätegruppe eingebunden?

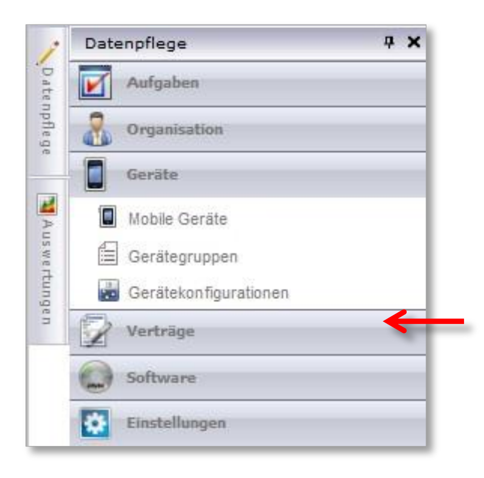


Abbildung 39 – Menüpunkt „Gerätekonfiguration"

Für das Erstellen einer neuen Gerätekonfiguration (in diesem Beispiel für iOS Geräte) führen Sie bitte die folgenden Schritte durch:

1. Aktivierung des Feldes „Gerätekonfiguration hinzufügen". Wählen Sie „iOS" und gehen Sie in diesem Beispiel auf „iOS Restriktionen".

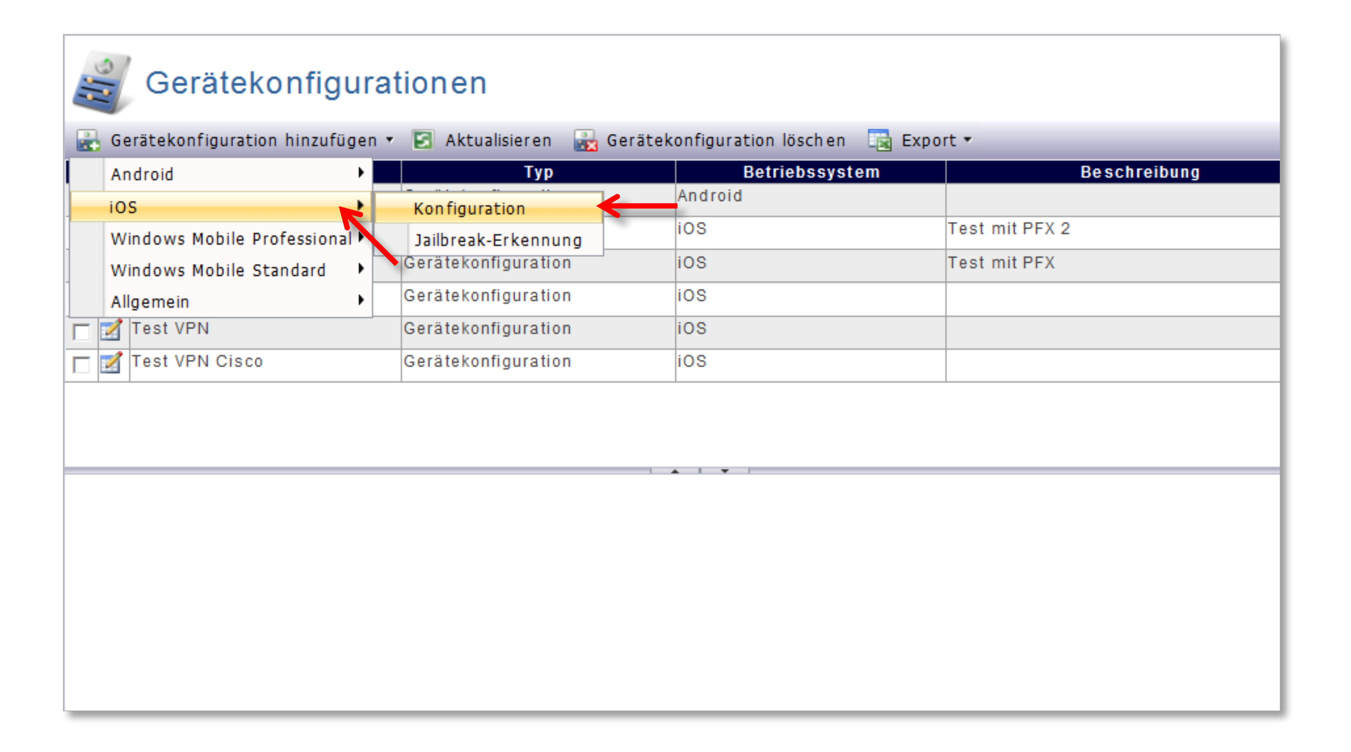


Abbildung 40 - Gerätekonfigurationen



2. Eingabe eines Namens und Beschreibung, Aktivierung/Deaktivierung von Gerätefunktionalitäten und Aktivierung des Feldes „Speichern"

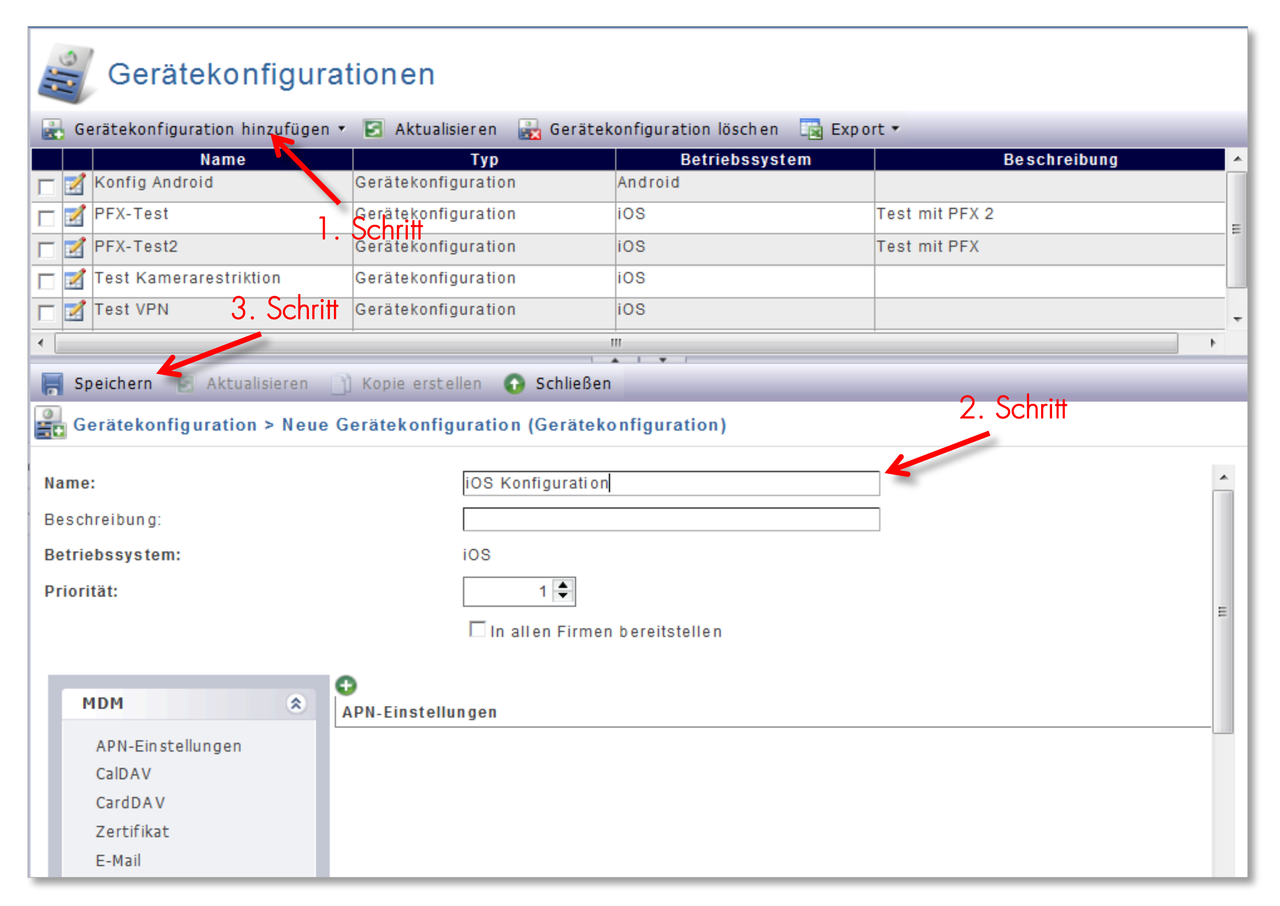


Abbildung 41 - Gerätekonfigurationen 3



3. Die erstellte Gerätekonfiguration ist nun gespeichert und kann bearbeitet, versendet oder gelöscht werden. Falls sie die Gerätekonfiguration in einer leicht abgeänderten Fassung für eine andere Gruppe benötigen, so können Sie diese mit der Schaltfläche „Kopie erstellen" kopieren und die Kopie anschließend verändern.
4. Im nächsten Schritt wechseln Sie bitte in den Bereich „Gerätegruppen".

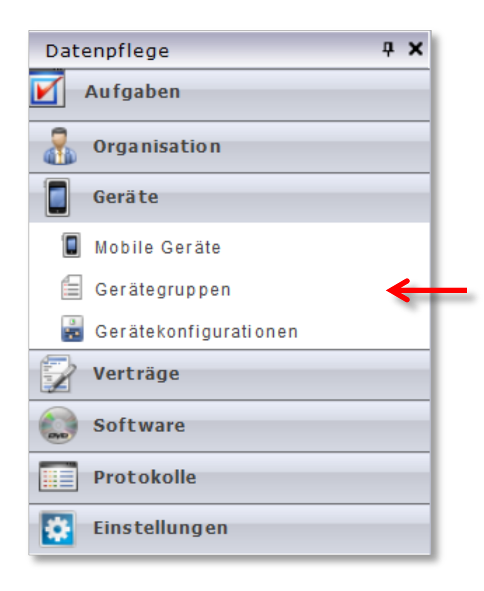
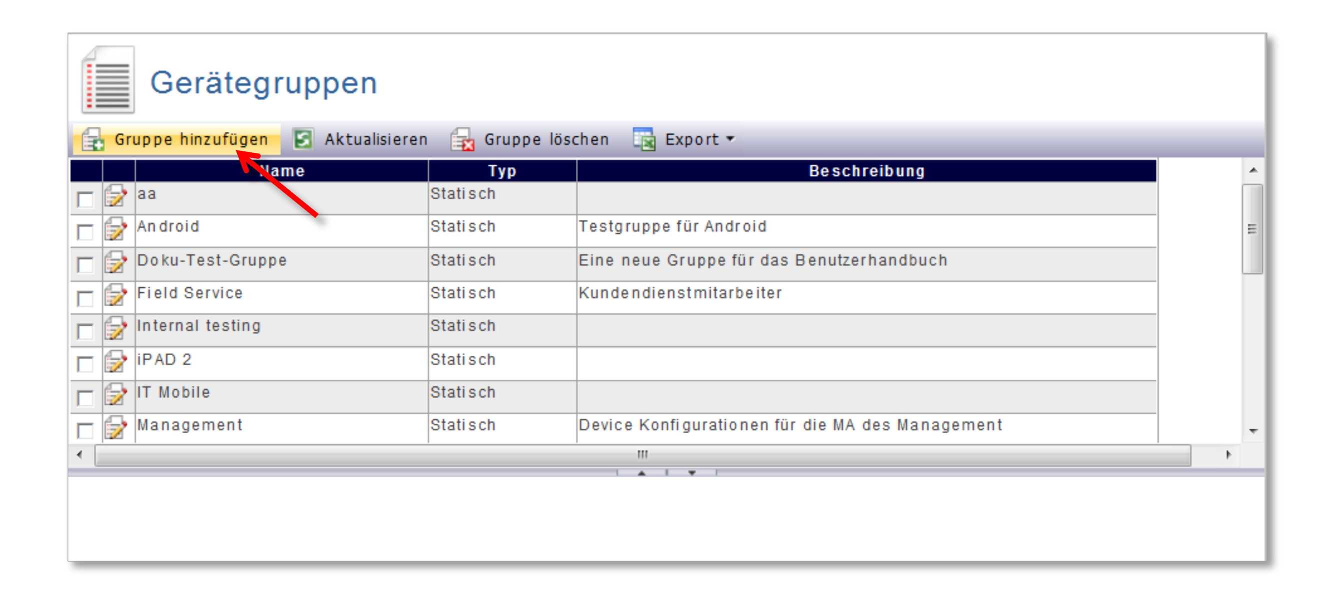


Abbildung 42 – Menüpunkt „Gerätegruppen"

5. Aktivieren Sie das Feld „Gruppe hinzufügen" und vergeben Sie einen neuen Namen.



Name	Typ	Beschreibung
aa	Statisch	
Android	Statisch	Testgruppe für Android
Doku-Test-Gruppe	Statisch	Eine neue Gruppe für das Benutzerhandbuch
Field Service	Statisch	Kundendienstmitarbeiter
Internal testing	Statisch	
iPAD 2	Statisch	
IT Mobile	Statisch	
Management	Statisch	Device Konfigurationen für die MA des Management

Abbildung 43 - Gerätegruppen 1

6. Wechseln Sie auf den Reiter „Gerätekonfigurationen“, markieren Sie die zuvor erstellte Gerätekonfiguration und verschieben diese mit Hilfe des Pfeil-Feldes von links nach rechts und aktivieren das Feld „Speichern“. Die Gerätekonfiguration ist nun der Gruppe zugeordnet und die Gruppe gespeichert.

Abbildung 44 - Gerätegruppen 2

3.5.2 Wie wird ein Benutzer in eine Gerätegruppe eingefügt, um die Einstellungen an das mobile Gerät zu übertragen?

Folgende Schritte sind durchzuführen, um einen Benutzer einer Gerätegruppe hinzuzufügen:

1. Wechseln Sie in den Bereich „Organisation“ und zum Unterpunkt „Mitarbeiter“.

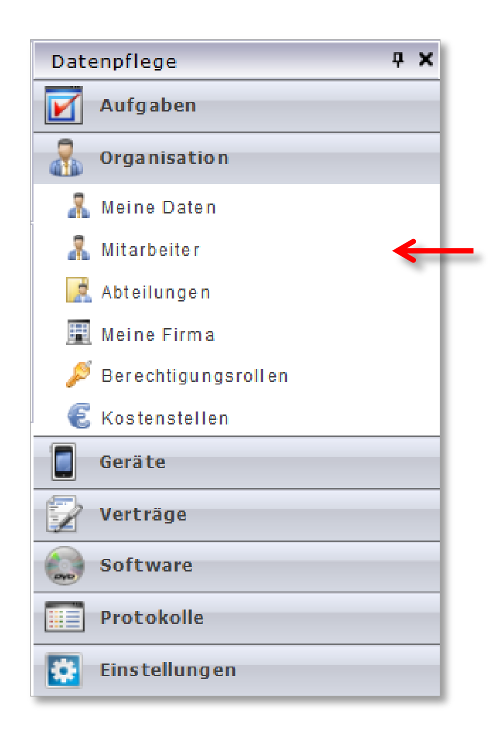


Abbildung 45 – Menüpunkt „Mitarbeiter“

2. Aktivieren Sie das Feld „Bearbeiten“ des gewünschten Mitarbeiters.
3. Wählen Sie im Menü „Standard Gerätegruppe“ die entsprechende Gruppe aus und aktivieren das Feld „Speichern“.

Abbildung 46 - Benutzer zur Gerätegruppe

4. Die Einstellungen werden automatisch in definierten Intervallen (siehe Abschnitt 2.7.1) übertragen. Weitere Schritte sind nicht nötig.
5. Für die sofortige Übertragung an das mobile Gerät führen Sie bitte die folgenden Schritte durch: Wechseln Sie in den Bereich „Geräte". Wählen Sie das gewünschte Gerät aus und aktivieren über das Feld „Gerätebenachrichtigung" den Punkt „Sende Einstellungen":

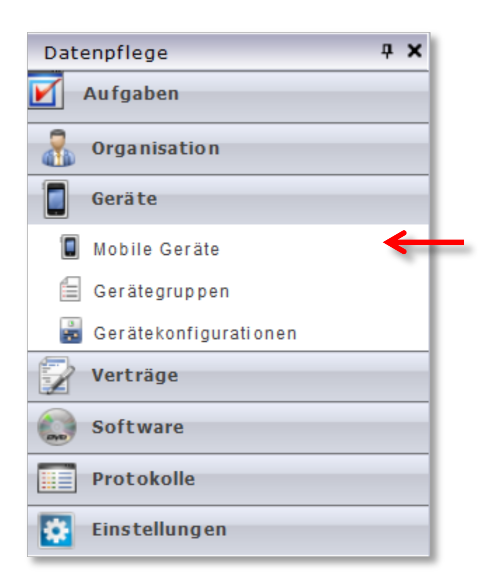


Abbildung 47 – Menü „Mobile Geräte"

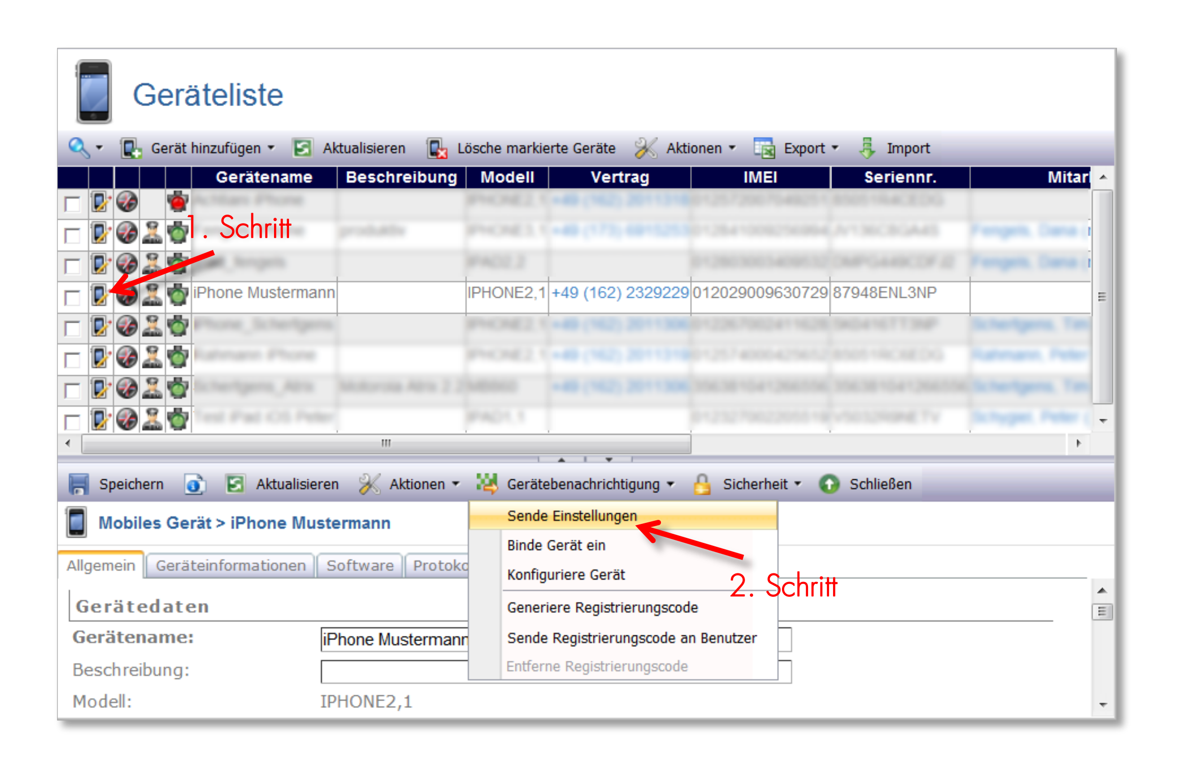


Abbildung 48 - Gerät einbinden 1

6. Die Daten werden im Hintergrund an das Gerät übertragen. Der Benutzer hat hier keine Möglichkeit, bzw. Bedarf, zur Interaktion.



3.5.3 Wie wird die E-Mail-Synchronisation eingerichtet?

Die Nutzung von Active Sync Accounts auf den mobilen Geräten gehört zu den Standards im Mobile Device Management. Durch die Einrichtung eines Active Sync Accounts werden die PIM-Daten (E-Mails, Kontakte, Termine) zwischen dem mobilen Gerät und dem Mail-Account des Benutzers im Unternehmen synchronisiert. Dies wird auch mit pureMDM abgebildet.

Durch die Systemvariablen für Domäne und Benutzer werden automatisch die entsprechenden Exchange-Einstellungen auf den mobilen Geräten gesetzt.

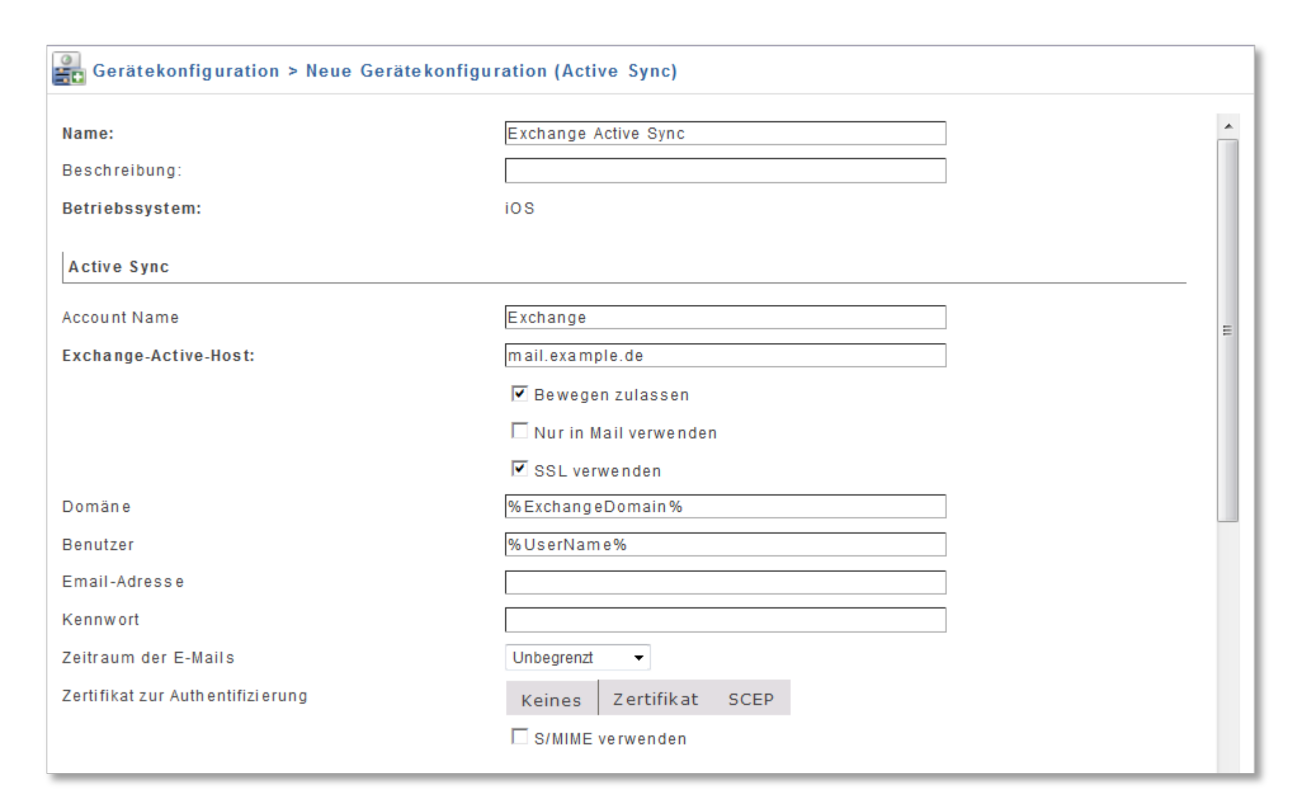


Abbildung 49 -- Exchange Active Sync

Sie können die Konfiguration für einen Exchange Active Sync Account in der Gerätekonfiguration über den Menüpunkt „Gerätekonfiguration hinzufügen" und den Unterpunkt „Exchange Active Sync" einrichten. Anschließend ist eine Gerätegruppe hinzuzufügen und die mobilen Geräte dieser Gerätegruppe mit den entsprechenden Einstellungen „over-the-Air" einzurichten. Der Benutzer bekommt auf dem mobilen Gerät die Aufforderung sein E-Mail-Passwort einzugeben. Nachdem er das Passwort eingegeben hat ist Active Sync eingerichtet, wodurch die PIM-Daten Synchronisation aktiviert wird.

3.6 Kann Software auf die mobilen Geräte verteilt werden?

Mit Hilfe von pureMDM und dem Afaria Client können Sie Software bereitstellen und auf die mobilen Geräte verteilen. Grundsätzlich ist hier zwischen Software aus dem App Store von Apple und Eigenentwicklungen (Enterprise Anwendung) zu unterscheiden.

Für Software aus dem App Store wird mit Hilfe des Afaria Clients auf dem iOS Gerät eine Weiterleitung zum App Store zur Verfügung gestellt.

Eigenentwicklungen (Enterprise Anwendung) können mit Hilfe des Afaria Clients auf dem iOS Gerät direkt zur Installation bereitgestellt werden. Hierzu erhält der Benutzer eine Push-Benachrichtigung über bereitgestellte Enterprise Apps.

Für die Installation des Afaria Clients auf dem mobilen Gerät suchen Sie im App Store von Apple nach „Afaria" und installieren dieses App:

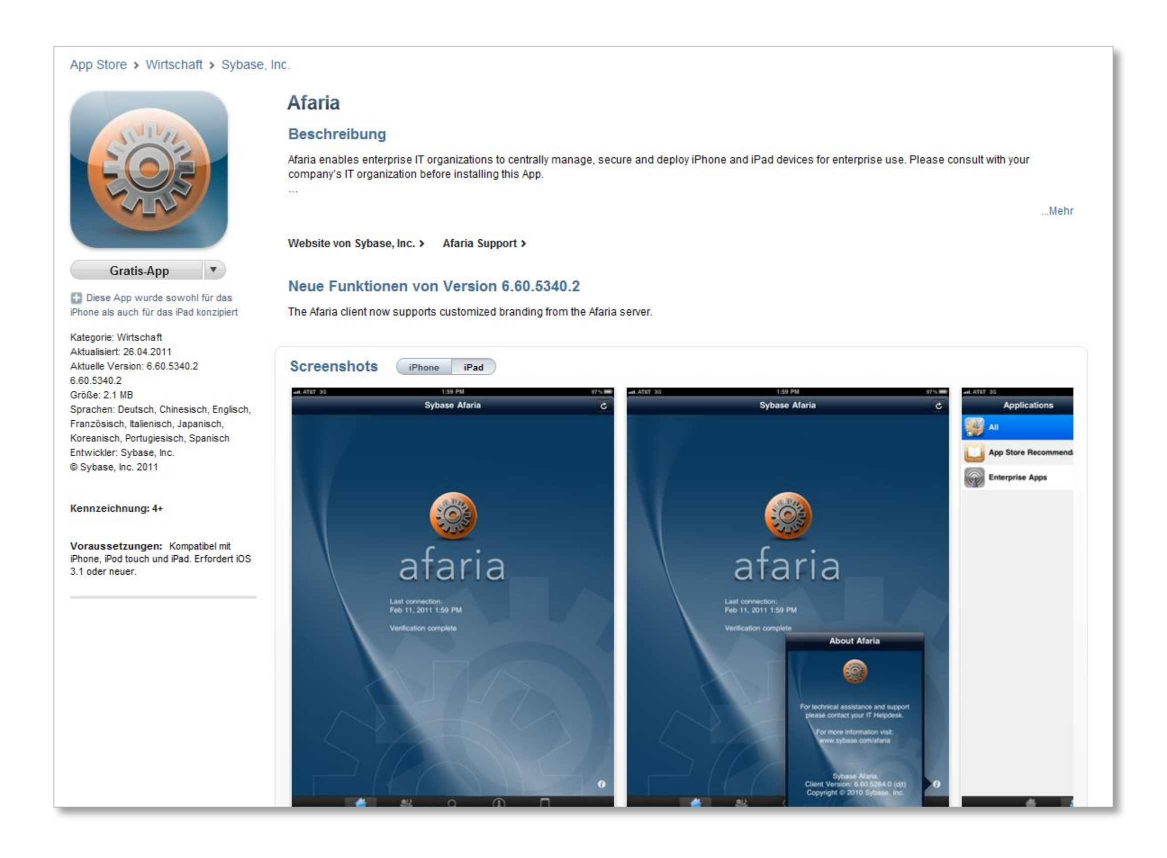


Abbildung 50 - Software, Afaria Client

3.6.1 Wie werden iOS App Store Anwendungen in pureMDM hinzugefügt?

Im Folgenden werden die Schritte zur Bereitstellung von iOS App Store Software über pureMDM beschrieben. Grundsätzlich muss erst die gewünschte Software hinzugefügt und im nächsten Schritt einer Gerätegruppe zugeordnet werden. Für alle Benutzer der ausgewählten Gerätegruppe wird somit eine Empfehlungsliste von Programmen auf dem mobilen Gerät zur Verfügung gestellt.

1. Wechseln Sie in den Bereich „Software", Unterpunkt „Software", wählen das Feld „Software hinzufügen", füllen Sie die Felder „Name" und „Beschreibung" aus und wechseln Sie den „Typ" von „iPhone Enterprise Anwendung" auf „iPhone App Store Anwendung":

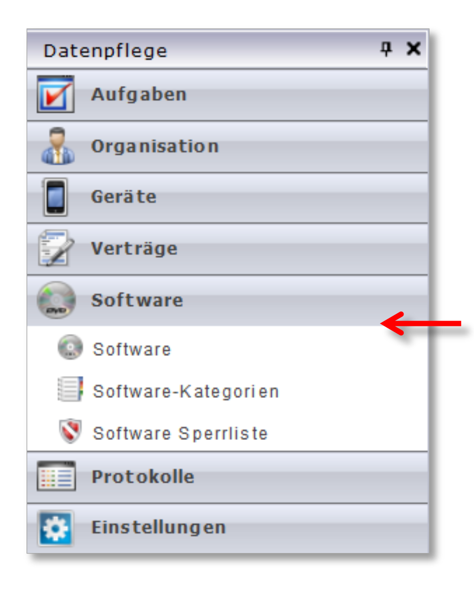


Abbildung 51 – Menüpunkt „Software"

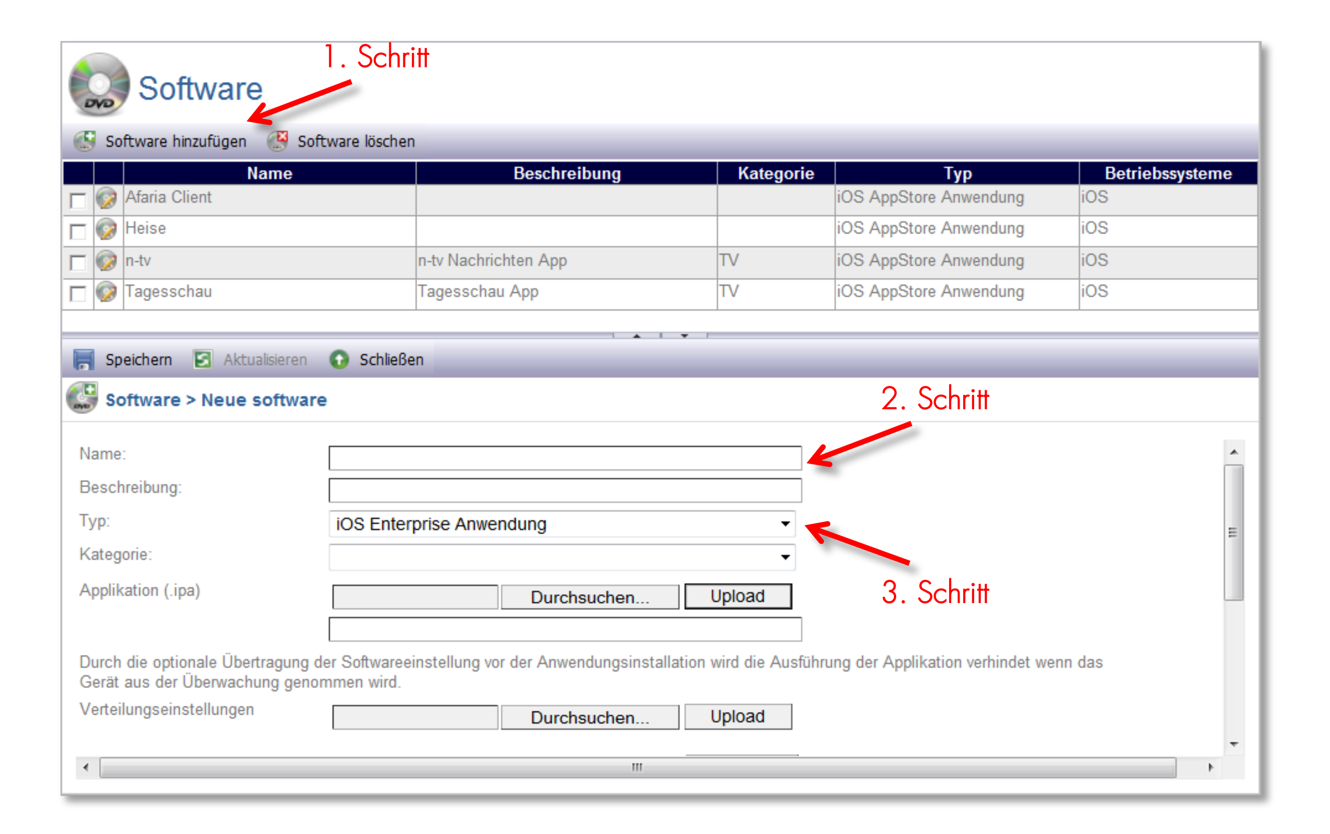


Abbildung 52 - Software hinzufügen 1

2. Die für das Feld „App Store-Nummer“ benötigte ID, ermitteln Sie indem Sie den folgenden Link öffnen und die gewünschte Software auswählen:
   http://itunes.apple.com/us/genre/mobile-software-applications/id6000?mt=8&letter=M&page=3#page
3. Die notwendige Nummer kopieren Sie bitte aus der, in der Adressleiste (Zahlenfolge hinter „id“) Ihres Internet-Browsers angezeigten URL. In unserem Beispiel verwenden wir die „heise.de“-App:

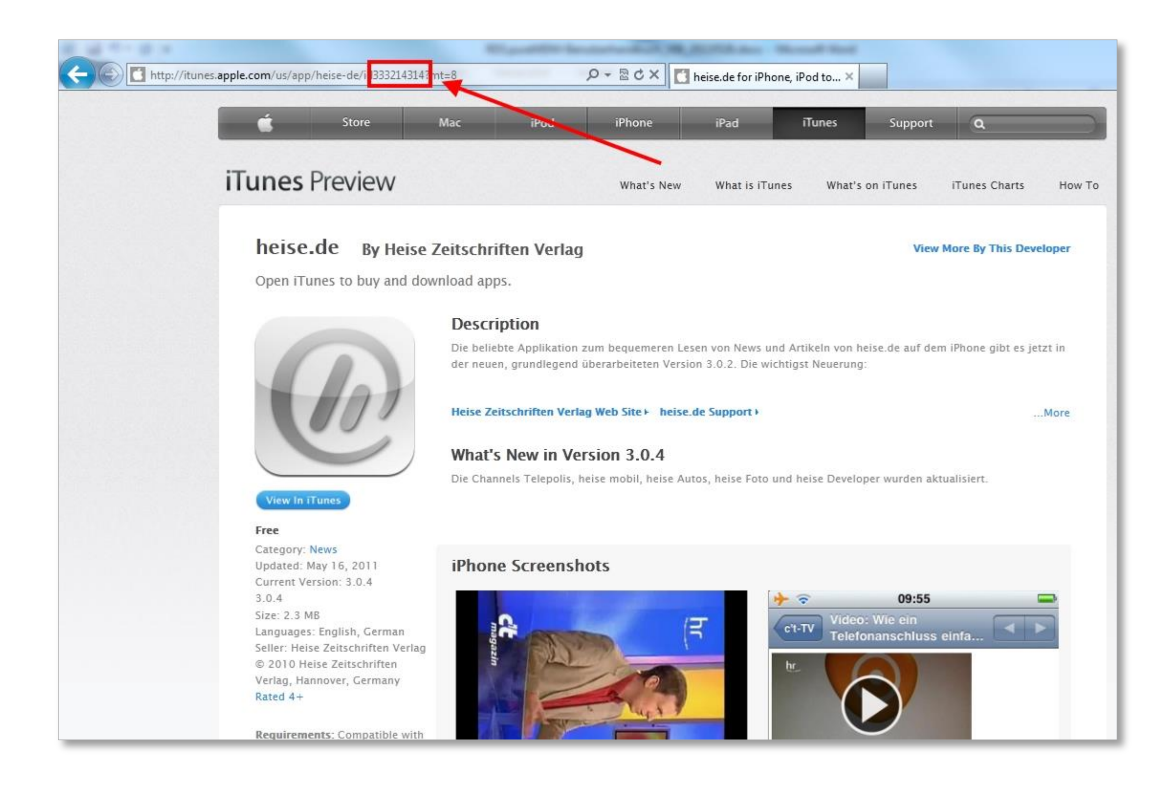


Abbildung 53 - Software hinzufügen 2

4. Fügen Sie diese Nummer im Feld „App Store-Nummer" ein. Sobald Sie in ein anderes Feld wechseln, wird die eingefügte Nummer überprüft und entsprechende Details angezeigt:

Software

Software hinzufügen | Software löschen

Name	Beschreibung	Kategorie	Typ	Betriebssysteme
AfariaClient	Afaria Client Software	Device Management	iOS AppStore Anwendung	iOS
AroundMe	Informationen rund um den aktuellen Standort	General	iOS AppStore Anwendung	iOS
BatteryStatus1	RDSAPP	TestEnterprise	iOS Enterprise Anwendung	iOS
DB Navigator	DB Navigator - The route planner for public transport!	Productivity	iOS AppStore Anwendung	iOS
Heise	Mobiles App von Heise	News	iOS AppStore Anwendung	iOS

Speichern | Aktualisieren | Schließen

Software > Heise

Name: Heise
Beschreibung: Mobiles App von Heise
Typ: iOS AppStore Anwendung
Kategorie: News
AppStore-Nummer: 333214314
App identifier: de.heise.news4
z.B. "com.sybase.afariaclient"

1. Schritt

de.heise.news4

2. Schritt

Applikationsdetails

heise.de (By Heise Zeitschriften Verlag)

AppStore

Description:
Die beliebte Applikation zum bequemeren Lesen von News und Artikeln von heise.de auf dem iPhone gibt es jetzt in der neuen, grundlegend überarbeiteten Version 3.0.2. Die wichtigsten Neuerungen:

1. Mac & i, die neue Themensite rund um Apple bei heise online. Siehe www.mac-and-i.de.

2. c't-TV

Als neuer Channel kommt c't-TV mit den beliebten Fernsehsendungen des c't magazins hinzu, moderier...

Price: Free
Category: News
Updated: Jul 21, 2011

Abbildung 54 - Software hinzufügen 3

5. HINWEIS: Um die Software überwachen zu können (u.a. für Whitelisting; Empfehlungsliste), ist der App-Identifier zwingend notwendig. Diesen erhalten Sie erst nach der Installation der entsprechenden App auf einem Gerät.
    a. Bitte installieren Sie die Software, die Sie verwalten möchten auf ein ausgerolltes Gerät.
    b. Bitte wählen Sie im Anschluss das entsprechende Gerät aus und suchen Sie die App unter dem Register „Software" in pureMDM.

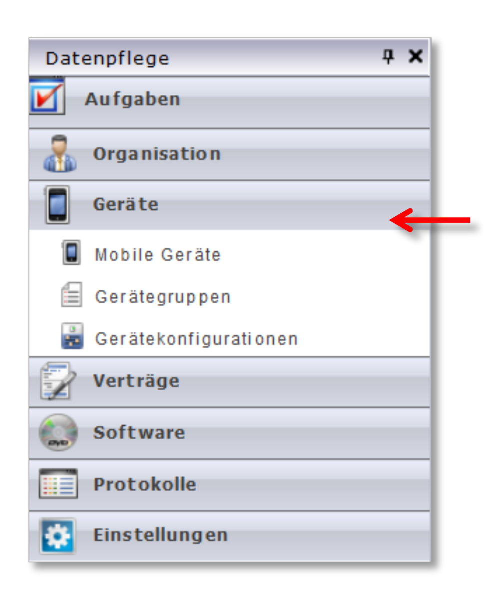


Abbildung 55 – Menüpunkt „Mobile Geräte"

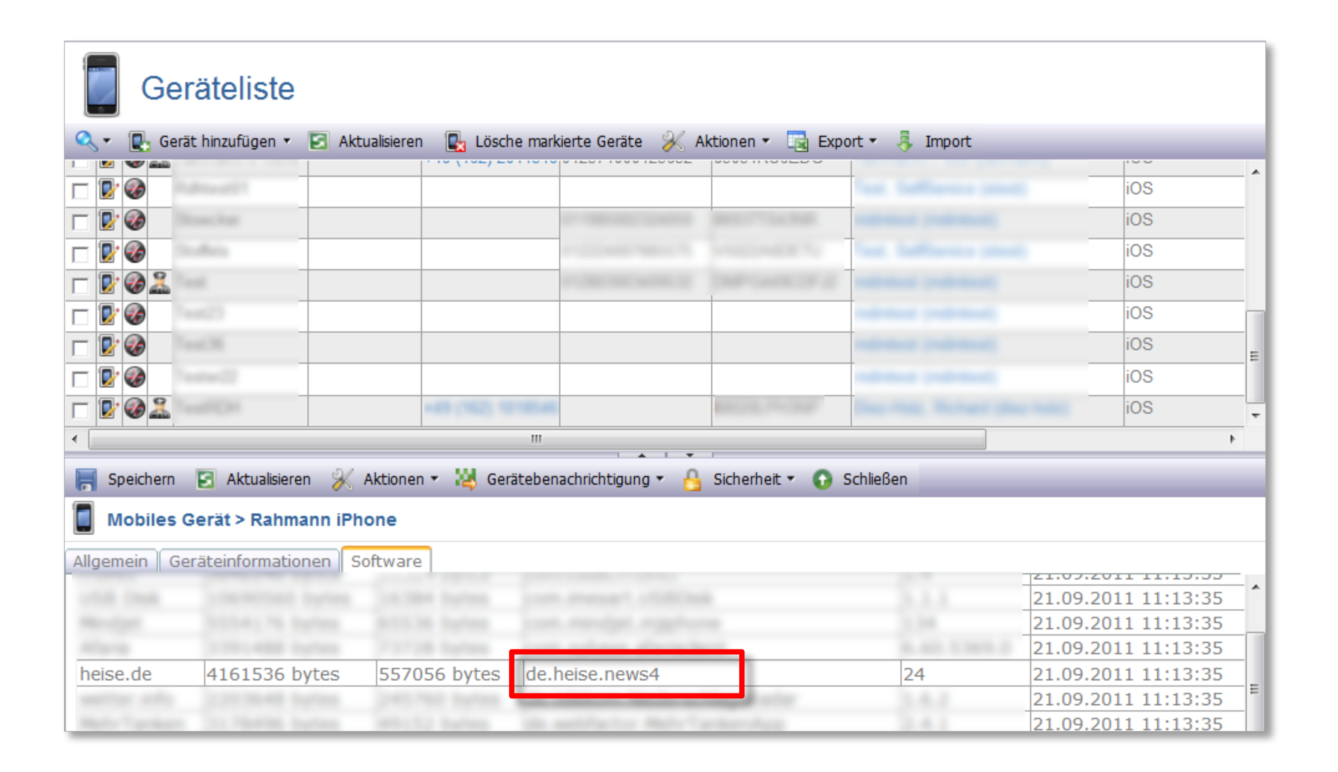


Abbildung 56 - Identifier

c. Bitte übertragen Sie den dort angezeigten Identifier (hier z.B. de.heise.news4) in das Feld für den App Identifier unter Software (Abbildung 71).

6. Aktivieren Sie das Feld „Speichern".

3.6.2 Wie werden Google Play Anwendungen in pureMDM hinzugefügt?

Die Methodik, Einträge für Google Play Apps zu erstellen, ähnelt derer für Apple App Store Apps.

a. Rufen Sie zuerst den Google Play über die URL https://play.google.com/store auf und suchen Sie nach der gewünschten App.

b. Kopieren Sie die App-ID, welche in der URL zwischen Strings „id=" und „&feature=" angezeigt wird.

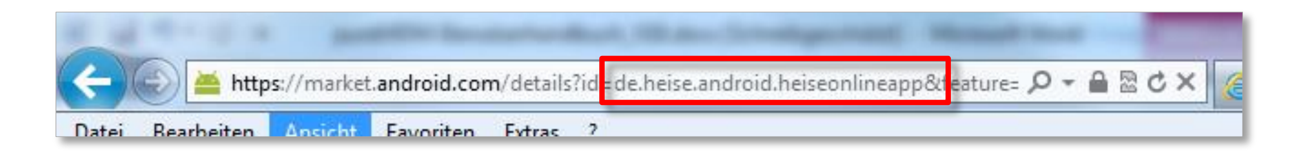


Abbildung 57 – Ermittlung der App-ID

c. Fügen Sie sie in pureMDM in das Feld „Paketname“ ein. pureMDM ruft die Daten der App automatisch ab und zeigt diese im unteren Bereich des Fensters an.

Abbildung 58 – Eintragen der App-ID

d. Vergeben Sie einen Namen, gegebenenfalls eine Beschreibung und Kategorie, und speichern Sie den Eintrag.

3.6.3 Wie kommt die Software auf das mobile Gerät?

Im Anschluss muss die gerade erstellte Software einer Gerätegruppe hinzugefügt werden damit diese mit Hilfe des Afaria Clients auf dem mobilen Gerät zur Verfügung gestellt werden kann.

Die folgenden Schritte sind zur Bereitstellung der Software/Verlinkung auf dem mobilen Gerät notwendig.

1. Wechseln Sie in den Bereich „Geräte"/"Gerätegruppen", wählen Sie die gewünschte Gerätegruppe zur Bearbeitung aus. Wählen Sie dann den Reiter „Software", markieren die Software und verschieben diese mit Hilfe der Pfeilfelder von der linken auf die rechte Seite der Tabelle:

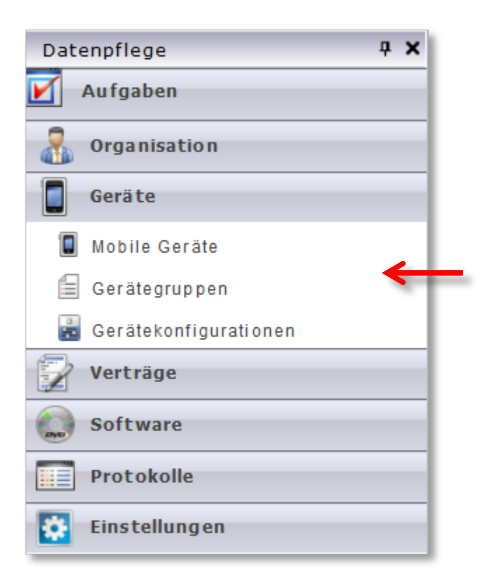


Abbildung 59 – Menüpunkt „Gerätegruppen"

Gerätegruppen

Gruppe hinzufügen | Gruppe löschen | Export

Name	Typ	Beschreibung
Finanzen	Statisch	
iOS 5	Statisch	iOS 5 Beta 7
IT Gruppe	Statisch	
Management	Statisch	Gerätegruppe
Marketing	Statisch	
Mustergruppe	Statisch	Eine Mustergruppe. An exemplary group.
Vorstand	Statisch	

1. Schritt

Speichern | Aktualisieren | Gerätebenachrichtigung | Schließen

2. Schritt

Gruppe > Mustergruppe

Allgemein | Gerätekonfigurationen | Software

Alle Software

Afaria Client
n-tv
Tagesschau
Heise

Zugeordnete Software

3. Schritt

4. Schritt

>>

<<

Abbildung 60 - Software zur Gerätegruppe 1

2. Die ausgewählte Software ist nun im Bereich „Zugeordnete Software“ hinterlegt. Aktivieren Sie das Feld „Speichern“.

Gerätegruppen

Gruppe hinzufügen | Gruppe löschen | Export

Name	Typ	Beschreibung
Finanzen	Statisch	
iOS 5	Statisch	iOS 5 Beta 7
IT Gruppe	Statisch	
Management	Statisch	Gerätegruppe
Marketing	Statisch	
Mustergruppe	Statisch	Eine Mustergruppe. An exemplary group.
Vorstand	Statisch	

2. Schritt

Speichern | Aktualisieren | Gerätebenachrichtigung | Schließen

Gruppe > Mustergruppe

Allgemein | Gerätekonfigurationen | Software

1. Schritt

Alle Software: Afaria Client, n-tv, Tagesschau

Zugeordnete Software: Heise

>> <<

Abbildung 61 - Software zur Gerätegruppe 2

3. Die Software wurde erfolgreich der Gerätegruppe hinzugefügt und steht nach der Übertragung allen Benutzern dieser Gruppe mit Hilfe des Afaria Clients auf dem Gerät zur Verfügung.

3.6.4 Kann die Software in Kategorien aufteilen werden?

Zur Differenzierung der bereitgestellten Software können Kategorien angelegt werden.

1. Wechseln Sie bitte in den Bereich „Software“/„Software-Kategorien“.

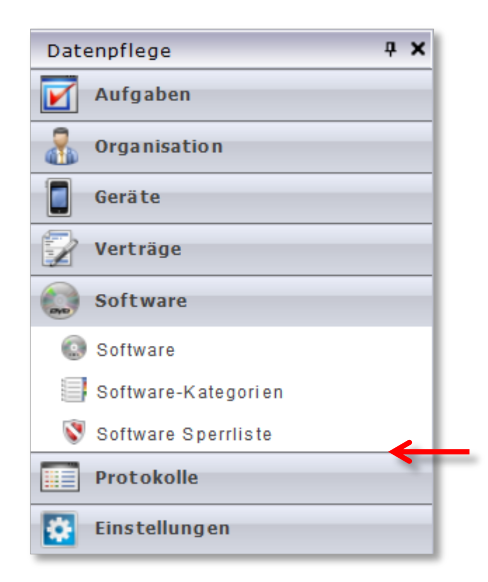


Abbildung 62 – Menüpunkt „Software-Kategorien"

2. Wählen Sie „Software-Kategorie hinzufügen", vergeben Sie einen Namen und aktivieren Sie das Feld „Speichern".

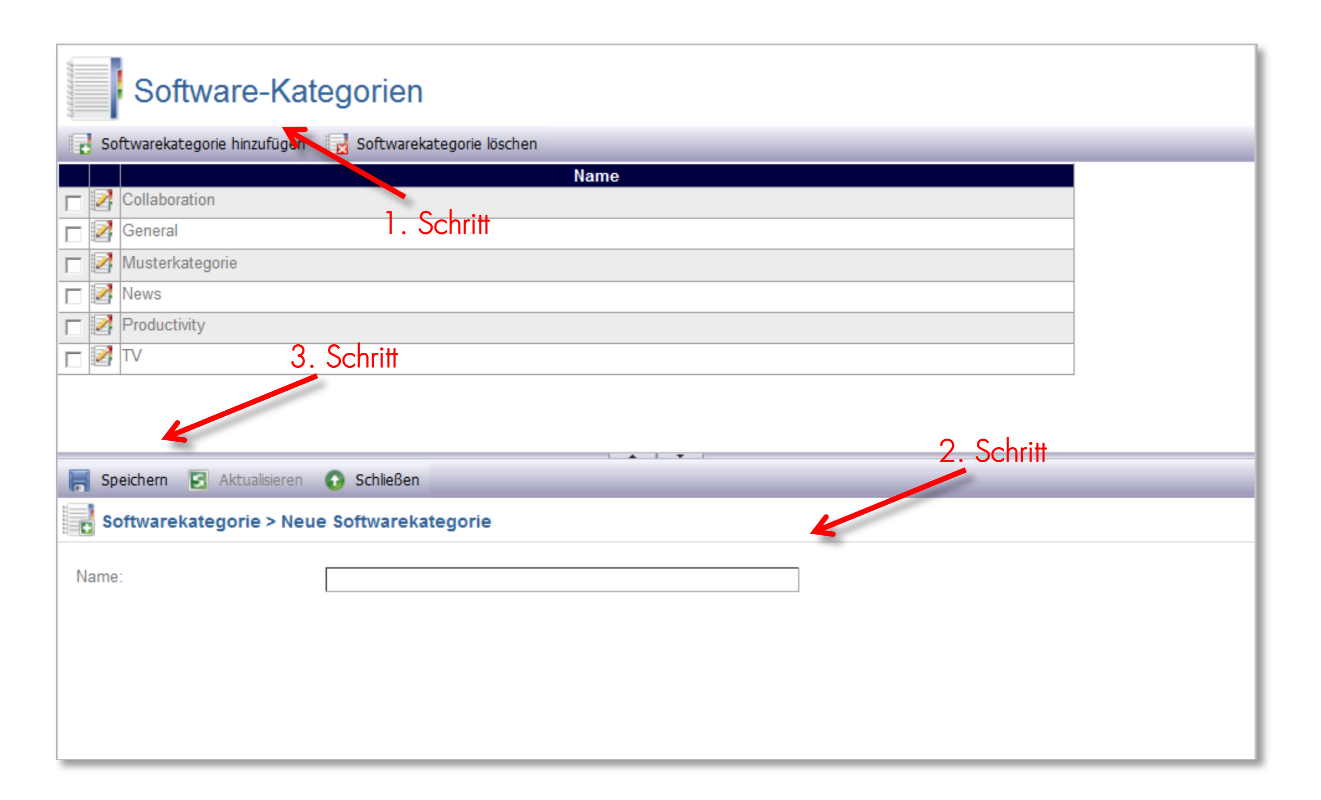


Abbildung 63 - Software-Kategorien 1



3. Sie können nun Software zum Punkt „Software-Kategorien" zuordnen.
   Gehen Sie dafür bitte in den Bereich „Software".

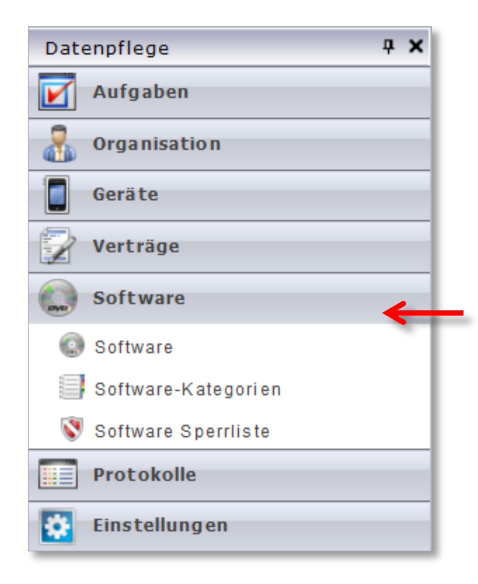


Abbildung 64 – Menüpunkt „Software"

4. Wechseln Sie in den Bearbeitungs-Modus der gewünschten Software und wählen im Feld „Kategorie" die gewünschte Zuordnung aus und aktivieren das Feld „Speichern".

Software

Software hinzufügen   Software löschen

	Name	Beschreibung	Kategorie	Typ	Betriebssysteme
	AfariaClient	Afaria Client Software	Device Management	iOS AppStore Anwendung	iOS
	AroundMe	Informationen rund um den aktuellen Standort	General	iOS AppStore Anwendung	iOS
	BatteryStatus1	RDSAPP	TestEnterprise	iOS Enterprise Anwendung	iOS
	DB Navigator	DB Navigator - The route planner for public transport!	Productivity	iOS AppStore Anwendung	iOS
	Heise	Mobiles App von Heise	News	iOS AppStore Anwendung	iOS
	Heise - Android		News	Android Market Anwendung	Android
	iBooks	Apple´s E-Book-Reader	General	iOS AppStore Anwendung	iOS

1. Schritt

Speichern   Aktualisieren   Schließen

Software > Heise

3. Schritt

Name: Heise
Beschreibung: Mobiles App von Heise
Typ: iOS AppStore Anwendung
Kategorie: News
AppStore-Nummer:
App identifier:

Collaboration
Device Management
General
News
Productivity
TestEnterprise

2. Schritt

Applikationsdetails

heise.de (By Heise Zeitschriften Verlag)   AppStore

Description:
Die beliebte Applikation zum bequemeren Lesen von News und Artikeln von heise.de auf dem iPhone gibt es jetzt in der neuen, grundlegend überarbeiteten Version 3.0.2. Die wichtigsten Neuerungen:

Abbildung 65 - Software-Kategorien 2

5. Die Software steht nach der Übertragung mit Hilfe des Afaria Clients sofort auf den mobilen Geräten in der zugeordneten Kategorie zur Verfügung.

3.7 Konfiguration von Workflows

Workflows dienen der automatischen Benachrichtigung von Administratoren und Anwendern sowie dem Ausführen von Aktionen sobald eine bestimmter Zustand eintritt.

Workflows funktionieren wie eine übliche Gerätekonfiguration (siehe Abschnitte 2.3.3.2 und 2.3.3.5). Sie werden angelegt und entsprechend

den Gerätegruppen zugewiesen. Voraussetzung ist, dass der Afaria Client auf dem mobilen Gerät installiert ist und vom MDM konfiguriert wurde.

In der Gerätekonfiguration „Jailbreak-Erkennung“ haben Sie die Möglichkeit eine Benachrichtigungs-E-Mail an den Benutzer und/oder an eine frei definierbare E-Mailadresse zu senden, wenn ein Jailbreak auf einem Gerät erkannt wurde. Weiterhin können automatische Aktionen ausgeführt werden, wie „Sperre Gerät“, „Entferne Daten aus Gerät“ oder „Entferne aus Gruppe und „Entferne Einstellungen aus Gerät“. Die entsprechende Android Gerätekonfiguration ist ähnlich aufgebaut. Hier ist die Option „Entferne Daten aus Gerät“ jedoch nicht verfügbar, da diese bei Android Geräten nicht möglich ist.

Das Erkennen eines SIM-Kartenwechsels funktioniert ähnlich der Jailbreak-Erkennung. Über die Gerätekonfiguration „SIM Karten Überwachung“ können Sie die gleichen automatischen Aktionen ausführen.



4 VERZEICHNISSE

4.1 Abbildungsverzeichnis